

Laid-Open No.,: 2003-0021859

The present invention relates to a method and system for providing a worm virus warning message and a worm virus vaccine to a client wireless communication apparatus on the propagation path of a worm virus. When a worm virus is detected in the wired/wireless Internet or an e-mail system, the propagation path of the worm virus is traced by a vaccine producer who made a vaccine against the worm virus, and a worm virus warning message and a worm vaccine are transmitted to the client wireless communication apparatus on the path of the trace automatically. In accordance with this invention, a worm virus host client which transmitted the worm virus to the system detected to be infected with the worm virus and the client which has received the worm virus can be cured. As a result, the infection of the worm virus can be minimized.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl. ⁷ G06F 17/00	(11) 공개번호 특2003-0021859 (43) 공개일자 2003년03월15일
(21) 출원번호 10-2001-0055313	
(22) 출원일자 2001년09월08일	
(71) 출원인 주식회사 비즈모델라인	
	서울특별시 강남구 역삼동 830-67 타호비즈니스센타
(72) 발명자 김재형	서울특별시 종로구 구기동 40동 익빌라 4-203
	김지한 서울특별시 서초구 반포 4동 미도아파트 307-701
	홍종철 서울특별시 관악구 신림 4동 466-39
	하연태 대전광역시 대덕구 신탄진동 고려아파트 208호

심사청구 : 없음(54) 무선 웜 바이러스 경고 메시지 자동 발송 방법 및 시스템**요약**

본 발명은 웜 바이러스(Worm Virus) 전파 경로에 위치하는 클라이언트 무선통신장치로 상기 웜 바이러스 경고 메시지 및 웜 백신(Worm Vaccine)을 제공하는 방법 및 시스템에 관한 것으로, 유·무선 인터넷 또는 전자 우편 시스템에서 웜 바이러스가 최초로 탐지되면, 웜 바이러스 백신 제작자에 의해 해당 웜 바이러스의 전파 경로를 추적하여 추적 경로에 위치하는 클라이언트 무선통신장치로 상기 웜 바이러스에 대한 경고 메시지 및 웜 백신을 자동 전송함으로써, 상기 웜 바이러스에 감염된 시스템으로 상기 웜 바이러스를 전송한 웜 바이러스 숙주 클라이언트 및 상기 웜 바이러스에 감염된 시스템으로부터 상기 웜 바이러스를 전송받은 웜 바이러스 수신 클라이언트의 웜 바이러스를 치료하여 상기 웜 바이러스에 의한 감염을 최소화시키는 방법 및 시스템에 관한 것이다.

대표도**도4****색인어**

바이러스, 경고메시지, 웜 백신, 무선통신장치

영세서**도면의 간단한 설명**

도1은 바이러스, 웜, 그리고 백도어로 구성된 웜 바이러스에 대한 간단한 블록도이다.

도2는 일반적인 웜 바이러스가 특정 컴퓨터를 감염시키고, 다른 컴퓨터로 자동 전파되는 과정에 대한 간단한 흐름도이다.

도3은 백신, 웜, 그리고 백도어로 구성된 웜 백신에 대한 간단한 블록도이다.

도4는 웜 백신이 웜 바이러스를 추적하는 단계에서, 웜 바이러스에 대한 웜 백신이 기존에 대해서, 2차에서 N차 웜 바이러스 감염자에게 감염자의 무선통신장치로 웜 바이러스 경고 메시지를 전송하여 주고 치료 여부를 확인한 후 웜 바이러스 감염자의 치료 요청에 따라 웜 백신을 전송하는 경우에 대한 간단한 블록도이다.

도5는 웜 백신이 웜 바이러스를 추적하는 단계에서, 1차에서 N차까지의 웜 바이러스 감염자에게 감염

자의 무선통신장치로 웜 바이러스 감염 사실을 전송하여 주고 치료 여부를 확인한 후, 웜 바이러스 감염자의 치료 요청에 따라 백도어를 이용하여 웜 바이러스를 추적하는 경우에 대한 간단한 블록도이다.

도면6은 웜 바이러스 1차 감염자로부터 상기 웜 바이러스 전파경로를 추출 및 상기 전파 경로에 위치하는 클라이언트 무선통신장치로 경고 메시지를 자동으로 발송하고 치료 여부를 확인한 후 웜 백신을 자동으로 발송하는 것에 대한 간단한 블록도이다.

도면7은 웜 바이러스 1차 감염자로부터 상기 웜 바이러스 전파 경로를 추출 및 상기 전파 경로에 위치하는 클라이언트 무선통신장치로 경고 메시지를 자동으로 발송하고 치료 여부를 확인한 후 웜 백신을 자동으로 발송하는 것에 대한 간단한 흐름도이다.

도면8은 외부와 차단된 가상 네트워크 안에서 웜을 찾는 웜 바이러스 검색부에 대한 간단한 블록도이다.

도면9는 상기 치료 여부 확인 감염자에게 전송된 웜 백신의 웜과 백도어를 통해 도면 7과 같은 각 단계들을 반복하여 웜 바이러스를 말살하는 과정에 대한 간단한 흐름도이다.

도면10은 웜 백신 개발자로부터 백신 메일링 서비스 요청자 또는 웜 바이러스 1차 감염자에게 전송된 웜 백신이 웜 바이러스를 치료하고 있는 간단한 예시도이다.

도면11은 2차 웜 바이러스 감염자의 무선통신장치로 웜 바이러스 감염 사실을 알리고 치료 여부를 확인하는 경고 메시지 발송의 일실시예도이다.

(도면의 주요부분에 대한 설명)

400 : 웜 바이러스 제작자	405 : 웜 백신 개발자
410 : 웜 바이러스 1차 감염자	415 : 웜 바이러스 2차 감염자
420 : 웜 바이러스 3차 감염자	425 : 이메일 서버
430 : 이동통신사	

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 유·무선 인터넷 또는 전자 우편 시스템에서 웜 바이러스가 최초로 탐지되면, 웜 바이러스 백신 제작자에 의해 해당 웜 바이러스의 전파 경로를 추적하여 추적 경로에 위치하는 클라이언트 무선통신장치로 상기 웜 바이러스에 대한 경고 메시지 및 웜 백신을 자동 전송함으로써, 상기 웜 바이러스에 감염된 시스템으로 상기 웜 바이러스를 전송한 웜 바이러스 속주 클라이언트 및 상기 웜 바이러스에 감염된 시스템으로부터 상기 웜 바이러스를 전송받은 웜 바이러스 수신 클라이언트의 웜 바이러스를 치료하여 상기 웜 바이러스에 의한 감염을 최소화시키는 방법 및 시스템에 관한 것이다.

웜은 단일 컴퓨터 시스템 내에서 프로그램 사이를 이동, 또는 네트워크를 통해 서로 다른 컴퓨터 시스템으로 자동 복제 전파되는 프로그램 조각이나 악성 코드로서, 컴퓨터 바이러스와 자주 혼동되지만 웜 자체가 컴퓨터 바이러스는 아니다.

컴퓨터 바이러스는 악의에 찬 목적을 가지고 기 전염된 컴퓨터 디스크에서 다른 컴퓨터 디스크로 자신을 복사하는 프로그램으로서, 컴퓨터 바이러스의 목적은 전염된 컴퓨터 디스크의 정보를 파괴하고, 시스템을 다운시키거나 비정상적으로 운영되도록 하는 것이다. 따라서 특정 컴퓨터에 접근하여 정보를 외부로 유출하는 백도어(Back Door)는 컴퓨터 바이러스가 아니다.

백도어는 특정 컴퓨터 시스템에 대하여 시스템 보안이 제거된 비밀 통로로서, 시스템 개발자 또는 서비스 기술자가 해당 시스템의 디버그나 유지 보수를 위해 정식 절차를 거치지 않고 시스템에 접근하도록 만들어 놓은 통로이다. 백도어는 웜이나 바이러스와 달리 악의적 목적으로 만들어진 것이 아니며, 해당 제품이 출시되기 전에 대부분의 백도어는 제거된다. 물론 일부 제품은 향후 서비스 지원을 위해 백도어를 제거하지 않고 출시하는 경우도 있지만, 이와 같은 경우에도 시스템 유지 보수를 위한 개발자나 서비스 기술자 이외에는 접근할 수 없도록 철저히 은닉된다.

그러나, 본 발명에서 다루는 백도어는 상기와 같은 전통적인 의미의 백도어가 아니라, 시스템을 공격하는 침입자가 아무런 인증 과정도 거치지 않고, 로그 기록도 남기지 않은 상태에서 목표 시스템에 접근하기 위한 수단으로 사용하는 악의적 목적의 백도어로서, 목표 시스템에 에이전트 형태로 자동 설치되어 시스템 정보를 외부로 누출시키거나, 시스템 공격자가 언제든지 목표 시스템에 악의적으로 접근할 수 있는 방법을 제공한다.

웜 바이러스는 종류에 따라 악간의 차이는 있지만, 일반적으로 웜, 바이러스, 그리고 백도어 등이 적절하게 결합된 형태의 바이러스로서, 웜을 통해 네트워크에 연결된 컴퓨터에 자동 전파되고, 바이러스를 통해 전파된 컴퓨터를 감염시켜 시스템을 파괴하거나 비정상적으로 운용되도록 한 후, 백도어를 통해 바이러스 개발자에게 목표 시스템의 시스템 정보를 전송하거나, 악의적으로 접근할 수 있도록 하는 프로그램이나 악성 코드로서, 주로 전자 우편을 통해 다른 컴퓨터로 전파되기 때문에 이메일 바이러스라고도 한다.

오늘날, 상기와 같은 웜 바이러스가 급속도로 확산된 이유는, 인프라 구조의 단일성, 웜 개발의 편리성, 단일 커뮤니케이션 메커니즘에 의한 네트워크 접속률 증가, 그리고 기업과 개인 사이의 동일 기술 사용 등이며, 각각에 대하여 설명하면 다음과 같다.

인프라 구조의 단일성은 컴퓨터의 하드웨어와 소프트웨어를 공급하는 기업이 점차적으로 독점화 되면서, 전 세계 거의 모든 컴퓨터가 동일한 구조로 이루어져 있다는 것이다.

예를 들어, 전 세계 대부분의 데스크탑 컴퓨터가 마이크로소프트(Microsoft)가 공급하는 윈도즈 계열의 운영 체제(Win3.1/95/98/NT/2000/XP)와 인텔 호환 CPU(Central Processing Unit)를 사용하고 있으며, 워크스테이션의 대부분은 썬 마이크로시스템즈(Sun Microsystems)가 공급하는 솔라리스(Solaris) 계열의 운영체제를 사용하고 있다.

따라서 데스크탑 컴퓨터를 대상으로 하는 웜 바이러스 개발자는 마이크로소프트사에서 공급하는 윈도즈 계열의 운영체제에서 작동하는 웜 바이러스를 개발하는 것만으로, 최고 전 세계 데스크탑 컴퓨터의 90%를 감염시킬 수 있다.

웜 개발의 편리성은 마이크로소프트가 윈도즈 계열(Win95 OSR 버전 이후)의 운영체제에 COM(Common Object Model)이라고 불리는 기술을 탑재하면서, COM을 이용하여 고급 개발자가 아니어도 쉽게 웜 바이러스를 개발할 수 있게 되었다는 것이다.

COM은 프로그램의 컴포넌트 객체들을 개발하고 지원하기 위한 하부 기반 구조로서, CORBA(Common Object Request Broker Architecture)에서 정의된 수준의 기능 제공을 목표로 하며, 컴포넌트 오브젝트 간의 인터페이스 교섭, 생명 주기 관리(오브젝트 제거 여부 판단), 라이선스, 이벤트 서비스 등을 제공한다. 즉, 웜 바이러스 개발자는 윈도즈 운영체제에서 사용되는 COM을 통해 하부 구조의 시스템 프로그래밍없이, 시스템을 조작할 수 있는 프로그램을 쉽게 개발할 수 있게 되었다.

예를 들어, 웜 바이러스 개발자는 COM을 통해 마이크로소프트사의 아웃룩이나 이메일 구조에 대한 전문적인 지식 없이도, 아웃룩을 통해 이메일을 자동으로 발송할 수 있는 매크로를 쉽게 생성할 수 있다.

단일 커뮤니케이션 메커니즘에 의한 네트워크 접속률 증가는 대부분의 인터넷 사용자들이 동일한 메커니즘을 통해 인터넷이나 전자 우편에 접근하기 때문에, 웜 바이러스가 제작된 지 수초에서 수분이면 전 세계 수백만명의 인터넷 사용자에게 웜 바이러스를 전파시킬 수 있다는 것이다.

인터넷이나 전자 우편에 접근하는 대부분의 인터넷 사용자들은 COM 기반의 커뮤니케이션 메커니즘을 이용하며, COM은 웜 바이러스 개발자에게 편의성도 제공하지만, COM이라는 동일한 구조를 통해 웜 바이러스를 급속도로 전파시킬 수 있는 방법을 제공한다. 경우에 따라 웜 바이러스에 감염된 클라이언트의 메일 서버는, 메일 클라이언트에서 웜에 의해 자동 발생되는 이메일 전송 요청으로 시스템이 폭주하거나 다운될 수도 있다.

기업과 개인 사이의 동일 기술 사용은, 웜 바이러스가 기업이나 개인을 가리지 않고 전파된다는 것이며, 특히 기업에 보관되어 있는 고객 주소록을 통해 웜 바이러스를 전파시키는 경우는 그 파괴력과 전파 속도가 상상을 초월한다.

도면1은 바이러스, 웜, 그리고 백도어로 구성된 웜 바이러스에 대한 간단한 블록도이다.

데스크탑 컴퓨터를 목표로 하는 웜 바이러스는 COM을 기반으로 프로그래밍이 가능한 비주얼 C++(Visual C++)이나 비주얼 베이직(Visual Basic)과 같은 고급 언어로 작성되며, 대부분의 웜 바이러스는 메일 메시지나 EXE 형태의 실행파일 또는 VBS 형태의 스크립트 등과 같은 첨부 파일의 형태로 제작된다. 이것은 기존 바이러스가 주로 어셈블리 언어(Assembly Language)와 같은 로우레벨 언어(Low Level Language)로 작성되었던 것과는 매우 다른 점이다. 즉, 그만큼 웜 바이러스 제작이 쉽고 간편할 뿐만 아

니라, 파괴력도 기존 바이러스에 비해 엄청나다는 것을 의미한다.

웜 바이러스는 종류에 따라 약간의 차이는 있지만, 기본적으로 바이러스, 웜, 그리고 백도어 등으로 구성되어 있으며, 이와 같은 웜 바이러스 구성요소는 독립 모듈별로 나뉜 것이 아니라, 웜 바이러스의 기능에 따라 구분한 것이다.

웜 바이러스의 바이러스는 COM을 기반으로 고급 언어로 작성되었기 때문에, 기존의 전통적인 바이러스가 파일의 엔트리 코드 부분을 감염시키는 것과는 달리, 지능적으로 파일의 중간 부분에 JTV(Jump To Virus) 명령어를 심어 놓으며, EPO(Entry Point Obscuring) 암호화 기법을 통해 바이러스가 시스템 제어권을 제일 먼저 얻어 암호를 해독한 후, 시스템을 감염시키도록 설정되어 있다.

따라서, 웜 바이러스가 메일 클라이언트에 수신되어 최초 실행되면, 바이러스는 Win32 커널을 스캐닝하여 운영체제의 종류, 레지스트리 구조, 현재 디렉토리와 시스템 디렉토리의 위치, 그리고 COM 버전과 메일 클라이언트 종류 등을 스캐닝하여 시스템 정보를 추출한 후, 웜 바이러스를 시스템 상의 특정 위치에 복제하고, 웜 바이러스에 포함되어 있는 웜과 백도어를 은닉시킨 후, 감염시킬 목표를 찾아 바이러스가 원하는 형태로 시스템을 감염시킨다.

일반적으로 바이러스가 목표로 하는 파일은 모든 윈도즈 계열 운영 체제에서 사용되는 원속(wsock32.dll)과 같은 시스템 파일과, COM을 지원하는 오피스 제품군(엑셀, 워드, 파워포인트 등)과 메일 클라이언트 응용프로그램(아웃룩, 아웃룩 익스프레스) 등이며, 특히 COM을 지원하는 응용프로그램들은 웜이 COM을 이용하여 자신을 다른 컴퓨터로 전파하기 쉽도록 변형한다.

웜 바이러스의 웜은 바이러스에 의해 시스템의 특정 위치에 복제된 후, 활동을 시작하며, 메일 클라이언트의 주소록과 받은 편지함, 보낸 편지함, 그리고 클라이언트가 방문하는 인터넷 웹사이트와 FTP 사이트 등을 참조하여 자신을 전파시킬 메일 주소를 추출한다. 이 때 웜이 어떠한 방식으로 메일 주소를 추출하는가는 웜 바이러스의 종류에 따라 달라지며, 일반적으로 바이러스 백신 도메인이나 백신 관련 조사 연구 기관의 도메인을 제외한 나머지 메일 주소를 추출한다.

상기와 같이 메일 주소의 추출이 완료되면, 웜은 추출된 메일 주소로 웜 바이러스를 포함한 메일을 전송한다. 특히, 일부 웜 바이러스는 추출된 메일 주소로 자신을 전파시킨 후, 바이러스에 의해 변형된 시스템 파일(wsock32.dll)을 다시 복구하여, 바이러스 감염 여부를 확인하지 못하도록 하는 경우도 있다.

웜 바이러스의 백도어는 웜과 같이 바이러스에 의해 시스템의 특정 위치에 복제된 후, 바로 활동을 시작하며, 일반적으로 웜과는 독립적으로 실행된다.

백도어 컴포넌트가 시스템에 설치되기 위해서는 윈도우 시스템 키가 생성된 후, 감염된 시스템 파일을 가리키도록 레지스트리를 변경해야 한다. 만약 이 때 시스템 키가 이미 존재하여 백도어를 시스템에 설치할 수 없다면, 백도어 컴포넌트는 레지스트리를 이용하여 다음에 부팅될 때 자동 설치하도록 조작한다.

일단 백도어가 설치되면, 웜 바이러스에 감염된 시스템은 특정 인터넷 서버로 연결되면, 웜 바이러스가 활동하기 위해 필요한 파일을 다운로드 하여 시스템을 다른 바이러스로 재감염 시키거나, 시스템 정보를 백도어가 지정한 서버로 전송한다.

웜 바이러스를 전파시키는 웜 전파 방법에는 자가(Native) 전파, 기생(Parasitic) 전파, 독단 프로토콜(Arbitrary Protocol) 전파, 그리고 P2P 전파 등이 있으며, 각각에 대하여 설명하면 다음과 같다.

자가 전파 방법은 웜 바이러스가 첨부 파일의 형태가 아니라 이메일 메시지로 전송되기 때문에, 메일 클라이언트가 웜 바이러스가 포함된 메일을 열지 않고, 메일 서버에서 메일 클라이언트로 이메일을 전송받는 것만으로 웜을 전파시키는 것이다.

기생 전파 방법은 웜 바이러스가 첨부 파일의 형태로 전송되는 것으로, 메일 클라이언트 사용자가 웜 바이러스가 감염된 이메일을 열어야만 웜을 전파시키는 것이다.

독단 프로토콜 전파 방법은 이메일 이외의 프로토콜을 전파 수단으로 이용하는 웜 바이러스 전파로서,

IRC (Internet Relay Chat) 프로토콜이나 FTP(File Transfer Protocol), 또는 TCP/IP 등과 같은 기존 인터넷 프로토콜을 통해 전파되는 것이다.

P2P 전파 방법은 독단 프로토콜 전파 방법의 일종으로, 최근 네스터나 소리바다와 같은 P2P 응용프로그램이 등장하면서, P2P 응용프로그램을 통해 웜 바이러스가 전파되도록 하는 것이다.

도면2는 바이러스, 웜, 그리고 백도어로 이루어진 일반적인 웜 바이러스가 특정 컴퓨터에 전파되어 바이러스를 감염시키고, 백도어를 설치한 후, 웜을 통해 다른 컴퓨터로 자동 전파되는 과정에 대한 간단한 흐름도이다. 단, 도면1은 일반적인 웜 바이러스에 대한 것이며, 바이러스 종류에 따라 순서 또는 방법 등이 다를 수 있다.

웜 바이러스 제작자 특정 이메일 주소로 웜 바이러스가 포함된 전자 우편을 전송하면, 이것은 이메일 주소에 해당하는 메일 서버에 전송되어 임시 저장된다. 이 때 웜 바이러스는 첨부 파일 또는 메일 메시지의 형태로 존재하며, 메일 클라이언트에서 POP3(Point Of Presence 3)나 IMAP(Internet Message Access Protocol) 등을 이용하여 클라이언트로 전송을 요청하면, 메일 서버는 주어진 프로토콜에 의해 해당 메일을 클라이언트로 전송한다.

메일 서버로부터 메일 클라이언트로 웜 바이러스가 포함된 메일이 수신되어 최초 실행되면, 웜 바이러스의 바이러스는 클라이언트가 웜 바이러스가 활동할 수 있도록 시스템 파일들을 변경하고, 자신을 시스템의 특정 영역에 복제하여 은닉한다.

상기와 같이 웜 바이러스가 복제되면, 웜 바이러스는 메일 클라이언트의 주소록이나 받은 편지함에서 웜을 통해 자동 전파할 메일 주소를 추출한다. 이 때 웜 바이러스는 모든 메일 주소로 전파되는 것이 아니라, 백신 개발 기업이나 바이러스 조사 기관과 같은 메일 주소에는 전파하지 않으며, 경우에 따라 받은 편지함 속에서 첨부 파일이 있는 메일 주소에만 선택적으로 전파하기도 한다. 따라서 웜 바이러스가 자신을 자동 전파하기 위해 추출하는 메일 주소의 종류는 웜 바이러스마다 약간씩 다르며, 추출하는 방법도 서로 다르다. 예를 들어, 멜리사 웜의 경우에는 메일 클라이언트 주소록의 상위 50개를 선택적으로 추출하며, 나비나드 웜의 경우에는 받은 편지함 중에서 첨부 파일이 있는 메일만을 선택적으로 추출한다.

웜에 의해 복제된 웜 바이러스를 전송한 메일 주소가 추출되면, 웜 바이러스는 추출된 메일 주소로 COM을 통해 SMTP(Simple Mail Transfer Protocol)로 하여금 웜 바이러스가 포함된 메일을 발송하도록 요청한다.

상기와 같이 추출된 메일 주소로 복제된 웜 바이러스가 전송되면, 해당 시스템에 복제된 웜 바이러스는 시스템에 백도어를 설치하여 바이러스 제작자가 해당 시스템에 접근할 수 있도록 처리하거나, 시스템 정보를 추출하여 바이러스 제작자에게 전송한다.

웜 바이러스에 의해 백도어 설치가 완료되면, 웜 바이러스는 최종적으로 바이러스를 통해 웜 바이러스에 감염된 시스템 악의적으로 조작한다. 특히 레지스트리를 변경하여 다음 번 부팅할 때마다 바이러스가 자동 실행되도록 하며, 경우에 따라서는 시스템을 파괴하는 경우도 있다.

따라서, 상기와 같은 과정을 통해 전파되는 웜 바이러스에 대하여, 네트워크에 연결된 컴퓨터의 웜 바이러스 안전 지대는 없으며, 웜 바이러스로부터 해방되는 근본적인 방법은 컴퓨터를 네트워크와 연결하지 않거나, 인터넷을 사용하지 않는 것이다. 그러나, 이와 같은 방법은 매우 위험한 것이며, 웜 바이러스 때문에 포기해야 하는 기회 가치가 너무나도 엄청나다.

현재까지 알려진 웜 바이러스 대처 방법은 메일 서버와 메일 클라이언트에서 이미 알려진 웜 바이러스에 대하여 필터링을 하거나, 컴퓨터에 웜 바이러스를 방어하고 감염된 바이러스를 치료할 수 있는 백신을 설치하는 것이다. 유일한 것이다.

그러나, 메일 서버 및 메일 클라이언트에서 이미 알려진 웜 바이러스에 대한 필터링을 통해 웜 바이러스를 차단하는 방법은 웜 바이러스의 속성상 거의 효과가 없으며, 신종 웜 바이러스에 대해서는 무방비 상태로 노출된다는 단점이 있다. 또한 네트워크에 연결된 컴퓨터에 백신을 설치하여 웜 바이러스를 차단하는 방법도, 메일을 읽을 때마다 백신을 가동해야 하는 불편함이 있으며, 아직 백신이 제작되지 않은 신종 바이러스에 대해서는 완전 무방비 상태가 된다는 심각한 단점이 있다. 특히 웜 바이러스의 전파 속도가 수초에서 수분이라는 특성상, 신종 바이러스에 무방비로 노출되는 기존 바이러스 차단 방법은 백신이 개발되거나 메일 서버에서 필터링을 해줄 때까지 웜 바이러스가 침입하지 않는 행운을 바라는 것과 다를 바가 없다.

발명이 이루고자 하는 기술적 과제

상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 유·무선 인터넷 또는 전자 우편 시스템에서 웜 바이러스가 최초로 탐지되면, 웜 바이러스 백신 제작자에 의해 해당 웜 바이러스의 전파 경로를 추적하여 추적 경로에 위치하는 클라이언트 무선통신장치로 상기 웜 바이러스에 대한 경고 메시지 및 웜 백신을 자동 전송함으로써, 상기 웜 바이러스에 감염된 시스템으로 상기 웜 바이러스를 전송한 웜 바이러스 숙주 클라이언트 및 상기 웜 바이러스에 감염된 시스템으로부터 상기 웜 바이러스를 전송받은 웜 바이러스 수신 클라이언트의 웜 바이러스를 치료하여 상기 웜 바이러스에 의한 감염을 최소화시키는 방법 및 시스템을 제공함에 있다.

발명의 구성 및 작용

본 발명은 웜 바이러스(Worm Virus) 전파 경로에 위치하는 클라이언트 무선통신장치로 상기 웜 바이러스 경고 메시지 및 웜 백신(Worm Vaccine)을 제공하는 방법 및 시스템에 관한 것으로, 유·무선 인터넷 또는 전자 우편 시스템에서 웜 바이러스가 최초로 탐지되면, 웜 바이러스 백신 제작자에 의해 해당 웜 바이러스의 전파 경로를 추적하여 추적 경로에 위치하는 클라이언트 무선통신장치로 상기 웜 바이러스에 대한 경고 메시지 및 웜 백신을 자동 전송함으로써, 상기 웜 바이러스에 감염된 시스템으로 상기 웜 바이러스를 전송한 웜 바이러스 숙주 클라이언트 및 상기 웜 바이러스에 감염된 시스템으로부터 상기 웜 바이러스를 전송받은 웜 바이러스 수신 클라이언트의 웜 바이러스를 치료하여 상기 웜 바이러스에 의한 감염을 최소화시키는 방법 및 시스템에 관한 것으로 웜 바이러스 감염후 즉각적인 처리를 위해 웜 바이러스 1차 또는 N차 감염자에게까지 감염자의 무선통신장치로 감염 사실을 전송하여 주고 치료 여부를 확인 및 웜 백신을 상기 감염자들의 무선통신장치로 전송하는 것이다.

유·무선 인터넷 또는 전자 우편 시스템에서 웜 바이러스가 최초로 백신 제작자에게 보고되면, 웜 바이러스 백신 제작자에 의해 해당 웜 바이러스의 전파 경로(상기 웜 바이러스에 감염된 시스템상의 이메일 주소록 및 받은 편지함, 보낸 편지함, 지운 편지함 등에서 추출한 이메일 주소를 통해 상기 웜 바이러스가 송·수신된 경로를 말하며, 상기 웜 바이러스에 감염된 시스템으로 상기 웜 바이러스를 전송한 웜 바이러스 숙주 시스템 및 상기 웜 바이러스에 감염된 시스템으로부터 상기 웜 바이러스를 전송받은 웜 바이러스 수신 시스템의 이메일 주소를 총칭함)를 추적하여 추적 경로에 위치하는 클라이언트 무선통신장치로 상기 웜 바이러스 경고 메시지 및 웜 백신(Worm Vaccine)을 즉각적으로 자동 전송함으로써, 상기 웜 바이러스에 의한 감염을 최소화하는 방법 및 시스템에 관한 것이다.

도면3은 백신(305), 명령 수신부(Order Receiver)(310), 웜(315) 그리고 백도어(320)로 구성된 웜 백신(300)에 대한 간단한 블록도이다.

웜 백신(300)은 웜 바이러스와 마찬가지로 메일의 메일 메시지 또는 첨부 파일의 형태로 전파되며, 백신(305), 웜(315), 명령 수신부(Order Receiver)(310) 그리고 백도어(320)로 구성되어 있다. 웜 백신(300)의 백신(305)은 웜 바이러스의 바이러스, 웜, 그리고 백도어를 치료하는 것이며, 웜 백신(300)의 웜(315)은 웜 바이러스의 전파 경로를 추적하는 것이고, 웜 백신(300)의 백도어(320)는 웜 백신의 웜에 의해서 추적된 웜 바이러스의 전파 경로를 백신 개발자에게 전송하여 백신 개발자로부터 웜 바이러스를 치료할 수 있는 최신 백신을 다운로드받도록 하는 것이다.

명령 수신부(Order Receiver)(310)는 웜 백신(300)내 웜의 자가 복제를 통해 웜 백신이 상기 웜 바이러스의 전파 경로로 전송되는 경우, 상기 웜 바이러스의 전파 경로를 추적하여 추적 경로에 위치하는 클라이언트 무선통신장치로 상기 웜 바이러스 경고 메시지를 전송한 후 상기 경고 메시지를 수신한 클라이언트 무선통신장치로부터 치료여부에 대한 응답 결과를 상기 백신 개발자로부터 전송 받아 상기 웜의 자가 복제를 통한 상기 웜 백신의 전송 경로를 선택적으로 선별하여 전송하도록 하는 역할을 한다.

웜 백신(300)의 백신(305)은 웜 바이러스에 노출된 시스템 또는 웜 바이러스에 이미 감염된 시스템에 웜 바이러스를 검색하고, 검색된 웜 바이러스를 치료하여 제거한 후, 웜 바이러스가 악의적으로 조작한 시스템의 변경사항을 원래대로 복구하는 역할을 수행한다. 웜 백신(300)의 백신은 웜 바이러스의 바이러스에 대해서만 치료와 복구를 수행하는 것은 아니며, 웜 바이러스의 바이러스, 웜, 그리고 백도어를 제거하고 치료하여 원래의 상태로 복구한다.

웜 백신(300)의 웜(315)은 웜 바이러스의 전파 경로를 추출하고, 추출된 웜 바이러스의 전자 경로에 대하여 상기 명령 수신부(310)에 수신된 백신 개발자(405)의 명령에 따라 웜 바이러스 감염자의 치료 요청에 대한 경로에 대해서 웜 백신(300)을 자가복제하여 상기 웜 바이러스 감염자의 치료 요청이 수신된 클라이언트 시스템으로 상기 웜 백신(300)을 전파시키는 역할을 수행한다.

웜 백신(300)의 백도어(320)는 웜 바이러스에 감염된 시스템에 최신 백신을 다운로드하거나, 현재 치료하는 웜 바이러스 이외의 새로운 신종 바이러스에 대한 치료 및 복구를 위해 필요한 조치를 취하기 위한

전통적인 목적의 백도어를 설치하는 역할을 수행한다. 웜 백신(300)의 백도어(320)는 웜 바이러스에 노출되었거나 감염된 시스템에서 추출된 웜 바이러스의 전파 경로 또는 웜 백신(300)이 전파되어야 할 경로 등을 백신 개발자에게 전달하는 역할을 수행한다.

웜 백신(300)이 웜 바이러스를 추적하여 치료하는 방법은, 웜 바이러스에 노출되었거나 감염된 시스템에서 웜 백신(300)이 전파될 경로를 결정하는 단계에 대하여 웜 바이러스가 전파된 경로 정보를 추출하는 경우와 웜 바이러스의 실제 전파 경로와 상관없이 웜 바이러스에 노출된 시스템에서 획득 가능한 모든 경로 정보를 추출하는 경우 등이 있으며, 웜 백신(300)이 웜 바이러스를 추적하는 단계에 대하여 웜을 통해 추적하는 경우와 백도어를 추적하는 경우, 그리고 웜과 백도어를 동시에 이용하여 추적하는 경우 등이 있다.

웜 백신(300)이 웜 바이러스를 추적하는 단계에서, 웜 백신(300)의 웜(315)을 이용하여 웜 바이러스를 추적하는 것은, 웜 바이러스에 대한 웜 백신(300)이 기 존재할 경우, 웜 백신(300)의 웜 안에 내장된 SMTP(Simple Mail Transfer Protocol)나 웜 바이러스에 노출되었거나 감염된 시스템의 SMTP를 이용하여 웜 백신이 웜 바이러스를 직접 추적하는 것이고(도4 참조), 웜 백신(300)의 백도어(320)를 이용하여 웜 바이러스를 추적하는 것은, 웜 백신(300)의 백도어(320)가 웜 바이러스에 노출되었거나 감염된 시스템에 백도어를 설치하고, 해당 시스템의 웜 바이러스 감염 정보와 웜 바이러스가 전파된 경로 정보 등을 백신 개발자에게 전송하면, 백신 개발자가 해당 시스템으로 직접 웜 백신(300)을 주입하여 치료하는 것이다. 그리고 웜 백신(300)의 웜(310)과 백도어(320)를 동시에 이용하여 웜 바이러스를 추적하는 것은, 상기 웜(310)을 이용한 추적과 백도어(320)를 이용한 추적을 결합한 형태로, 웜 백신(300)을 이용한 웜 바이러스의 추적을 웜 백신(300)에서 직접 사용할 수 있는 SMTP와 백신 개발자가 동시에 수행하는 것이다.

도면4는 웜 백신(300)이 웜 바이러스를 추적하는 단계에서, 웜 바이러스에 대한 웜 백신이 기 존재할 경우에 대해서, 2차에서 N차 웜 바이러스 감염자에게 감염자의 무선통신장치로 웜 바이러스 경고 메시지를 전송하여 주고 치료 여부를 확인한 후 웜 바이러스 감염자의 치료 요청에 따라 웜 백신을 전송하는 경우에 대한 간단한 블록도이다.

웜 바이러스 제작자(400)가 웜 바이러스를 유포하면(101), 이 웜 바이러스는 인터넷 상에서 웜 바이러스 1차 감염자(410)를 찾아 감염시키고,(102) 1차 감염자(410)로부터 다음 웜 바이러스 감염자 정보를 추출하여 2차 감염자(415)에게 웜 바이러스를 전파시키기 시작한다.(103) 이렇게 1차 감염자(410)로부터 전파되기 시작한 웜 바이러스는 2차 감염자(415)에게 전파되고,(103.1) 2차 감염자(415)는 1차 감염자(410)와 마찬가지로 웜 바이러스에 감염된다.(103.2) 웜 바이러스 2차 감염자(415)를 감염시킨 웜 바이러스는 2차 감염자(415)로부터 다음 웜 바이러스 정보를 추출하여, 해당 웜 바이러스에 대한 백신이 개발되어 감염된 모든 시스템이 치료되기 전까지 웜 바이러스 반복하여 재전파 된다.(103.3)

여기서, 1차 감염자라 함은 백신제공자에게 웜 바이러스 감염 여부를 문의하는 클라이언트를 의미하며, 본 발명에서 추구하는 웜 바이러스 경고메시지 및 웜 백신 자동 배포의 시발점 역할을 수행하는 것을 명기하는 바이다.

또한, 2차 감염자라 함은 상기 웜 바이러스에 감염된 1차 클라이언트 시스템으로 상기 웜 바이러스를 전송한 웜 바이러스 숙주 클라이언트 시스템 및 상기 웜 바이러스에 감염된 1차 클라이언트 시스템으로부터 상기 웜 바이러스를 전송 받은 감염 클라이언트 시스템을 총칭한다.

웜 바이러스에 감염된 1차 감염자(410)가 신종 웜 바이러스의 유포 사실을 웜 백신 개발자(405)에게 보고하면(104), 웜 백신 개발자(405)는 해당 웜 바이러스의 백신을 바이러스 1차 감염자(410)에게 전송한다(105).

웜 바이러스 1차 감염자(410)에게 전송된 웜 백신(300)은 해당 시스템을 치료하여 정상적인 상태로 복구한 후, 웜 바이러스의 감염 정보로부터 웜 백신(300) 전파 경로(상기 웜 바이러스에 감염된 시스템상의 이메일 주소록 및 받은 편지함, 보낸 편지함, 지운 편지함 등에서 추출한 이메일 주소를 통해 상기 웜 바이러스가 송·수신된 경로를 말하며, 상기 웜 바이러스에 감염된 시스템으로 상기 웜 바이러스를 전송한 웜 바이러스 숙주 시스템 및 상기 웜 바이러스에 감염된 시스템으로부터 상기 웜 바이러스를 전송받은 웜 바이러스 수신 시스템의 이메일 주소를 총칭함)를 결정하고, 웜 백신(300) 내의 백도어(320)를 이용하여 웜 바이러스의 전파경로를 웜 백신 개발자에게 전송한다(106).

웜 백신 개발자(405)는 각 E-mail사(425)와 연동하여 웜 백신(300)이 보내온 1차 감염자 E-mail의 주소록이나 1차 감염자(410)가 최근 사용한 E-mail 송/수신 주소로부터 2차 감염자 무선통신장치 전화번호를 다운 받는다(107)(사전 약정에 따라 E-mail서비스 신청서 작성시 사용자 무선통신장치 번호 입력란의 정보를 각 E-mail사(425)로부터 서비스 받는다).

여기서, 각 E-mail사(425)와 연동하여 2차 감염자 무선통신장치 전화번호를 다운받는 것은 본 발명 구현

의 간소화를 위한 것이며(각 E-mail사(425)는 E-mail 회원정보에 사용자 무선통신장치 번호를 기 저장하고 있으므로), 상기와 같이 2차 감염자 무선통신장치 전화번호 추출은 상기 1차 감염자(410)로부터 별도로 제공받거나 사전 서비스 제공을 위해 상기 1차 감염자 시스템내 이메일주소와 연동하는 무선통신장치 전화번호를 기 저장후 상기 주소록으로부터 상기 월 백신(300)에 의해 추출 가능한 바를 명기하는 바이다.

월 바이러스 감염자가 컴퓨터를 켜고 E-mail을 확인하기 전까지는 감염 사실을 모르기 때문에 감염자에게 즉각적으로 감염 사실을 알려 피해를 최소화하기 위해서 상기에 기술한 바와 같이 각 E-mail사(425)와 연동 또는 상기 1차 감염자로부터 별도로 제공받거나 사전 서비스 제공을 위해 상기 1차 감염자 시스템내 기 저장시킨 이메일주소와 연동하는 무선통신장치 전화번호를 추출하여 각 이동통신사(430)를 통해 도면 12와 같이 2차 월 바이러스 감염자의 무선통신장치로 월 바이러스 감염 사실을 알리고 치료 여부를 확인하는 경고 메시지를 발송한다(108).

2차 월 바이러스 감염자(415)가 치료를 요청하면 월 백신 개발자(405)는 상기 월 백신(300)내의 명령 수신부(오더 리시버, order-receiver)(310)를 사용하여 1차 월 바이러스 감염자(410)에게 기 전송 되어있는 월 백신(300)에게 2차 월 바이러스 감염자중 치료를 요청한 2차 월 바이러스 감염자(415)의 E-mail 주소를 전송하여(109) 월 백신(300)의 월(315)이 기 결정한 전파 경로를 수정하여 월 백신(300)이 치료를 요청한 2차 월 바이러스 감염자(415)에게 자동 전송되도록 한다(110).

상기와 같이 1차 감염자(410)로부터 전파되기 시작한 월 백신(300)이 월 바이러스를 추적하여 2차 감염자(415)에게 도달하면(110.1), 월 백신(300)은 월 바이러스에 감염된 2차 감염자(415)를 치료하여 복구하며(110.2). 이 과정은 월 바이러스를 추적하여 말살할 때까지 반복된다.(110.3)

월 바이러스 감염자의 시스템에 전송되어 있는 월 백신(300)과 백신 개발자(405)간의 명령/정보의 송·수신 방법은 월 백신(300)의 백도어(320)와 오더 리시버(310)를 사용하여 실현한다.

월 백신(300)은 월 바이러스 감염 정보로부터 월 백신 전파 경로를 결정하고, 상기 월 백신(300) 전파경로를 월 백신(300)내의 백도어(320)를 이용하여 백신 개발자(405)에게 전송한다.

백신 개발자(405)는 월 백신(300)의 백도어(320)로부터 전송 받은 월 백신(300)의 다음 전파 경로에 위치하는 월 바이러스 감염자중 치료를 요청한 감염자 정보만을 월 백신(300)내의 오더 리시버(310)로 전송하여 월 바이러스 치료를 요청한 감염자에게로만 전파되도록 한다.

도면5는 월 백신(300)이 월 바이러스를 추적하는 단계에서, 1차에서 N차까지의 월 바이러스 감염자에게 감염자의 무선통신장치로 월 바이러스 감염 사실을 전송하여 주고 치료 여부를 확인한 후, 월 바이러스 감염자의 치료 요청에 따라 백도어(320)를 이용하여 월 바이러스를 추적하는 경우에 대한 간단한 블럭도이다.

월 바이러스 제작자(400) 유포한 월 바이러스가 도면4의 101~103.x의 과정을 거쳐 전파되고, 1차 감염자(410)가 이 사실을 월 백신 개발자(405)에게 보고하면(104), 월 백신 개발자(405)는 해당 월 바이러스에 대한 백신을 개발한 후, 이것을 1차 감염자(410)에게 전송하여 월 바이러스를 치료하고, 1차 감염자(410)에 백도어(320)를 설치한다(105).

1차 감염자(410)에 설치된 백도어(320)는 1차 감염자(410)로부터 월 백신(300) 전파에 필요한 정보를 월 백신 개발자(405)에게 전송하고(106), 월 백신 개발자(405)는 각 E-mail사(425)와 연동 또는 상기 1차 감염자(410)로부터 별도로 제공받거나 사전 서비스 제공을 위해 상기 1차 감염자 시스템내 기 저장시킨 이메일주소와 연동하는 무선통신장치 전화번호 주소록을 이용하여 1차 감염자(410)가 최근 사용한 E-mail 송/수신 주소로부터 2차 감염자 무선통신장치 전화번호를 다운받는다(107).

월 바이러스 감염자가 컴퓨터를 켜고 E-mail을 확인하기 전까지는 감염 사실을 모르기 때문에 감염자에게 즉각적으로 감염 사실을 알려 피해를 최소화하기 위해서 상기에 기술한 바와 같이 각 E-mail사(425)와 연동 또는 상기 1차 감염자(410)로부터 별도로 제공받거나 사전 서비스 제공을 위해 상기 1차 감염자 시스템내 기 저장시킨 이메일주소와 연동하는 무선통신장치 전화번호 주소록을 이용하여 각 E-mail 사용자의 무선통신장치 번호를 서비스 받아 각 이동통신사(430)를 통해 도면 12와 같이 2차 월 바이러스 감염자의 무선통신장치로 월 바이러스 감염 사실을 알리고 치료 여부를 확인하는 경고 메시지를 발송한다(108). 2차 월 바이러스 감염자(415)가 치료를 요청하면 월 백신 개발자(405)는 직접 이 경로에 대하여 월 백신(300)을 전파시킨다(109).

월 백신 개발자(405)로부터 2차 감염자(415)에 전파된 월 백신(300)은, 해당 시스템을 치료한 후

백도어(320)를 설치하고(110), 이것은 2차 감염자(415)로부터 월 바이러스 경고 메시지와 월 백신(300) 전파에 필요한 정보를 추출하여 월 백신 개발자(405)에게 전송한다.(111)

2차 감염자(415)로부터 월 백신(300) 전파에 필요한 정보를 전송 받은 월 백신 개발자(405)는 이것을 바탕으로 E-mail사(425)와 연동 또는 상기 1차 감염자(410)로부터 별도로 제공받거나 사전 서비스 제공을 위해 상기 1차 감염자 시스템내 기 저장시킨 이메일주소와 연동하는 무선통신장치 전화번호 주소록을 이용하여 3차 월 바이러스 감염자(420)의 무선통신장치로 감염 사실과 치료여부를 확인하는 월 바이러스 경고 메시지를 전송하며, 감염자가 치료를 요청하면 3차 감염자(420)에게 월 백신을 전송하고,(112) 3차 감염자(420)에 도달한 월 백신(300)은 해당 시스템의 월 바이러스를 치료한 후, 백도어(320)를 설치한다(113).

이렇게 설치된 백도어(320)는 3차 감염자(420)로부터 월 바이러스 경고 메시지와 월 백신(300) 재전파에 필요한 정보를 추출하여 월 백신(300) 개발자(405)에게 전송하며(114), 이 과정은 인터넷 상에서 월 바이러스를 말살할 때까지 반복된다.

이하 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명한다. 단, 다음의 실시예는 본 발명을 가장 적절하게 설명하기 위한 여러 가지 방법 중 한 가지이며, 본 발명이 다음의 실시예로 한정되지는 않는다.

도면6은 월 바이러스 1차 감염자(백신제공자에게 월 바이러스 감염 여부를 문의하는 클라이언트를 의미하며, 본 발명에서 추구하는 월 바이러스 경고메일 및 월 백신 자동 배포의 시발점 역할을 수행하는 클라이언트)(410)로부터 상기 월 바이러스 전파 경로(상기 월 바이러스에 감염된 시스템상의 이메일 주소록 및 받은 편지함, 보낸 편지함, 지운 편지함 등에서 추출한 이메일 주소를 통해 상기 월 바이러스가 송수신된 경로를 말하며, 상기 월 바이러스에 감염된 시스템으로 상기 월 바이러스를 전송한 월 바이러스 속주 시스템 및 상기 월 바이러스에 감염된 시스템으로부터 상기 월 바이러스를 전송받은 월 바이러스 수신 시스템의 이메일 주소를 총칭함)를 추출 및 상기 전파 경로에 위치하는 클라이언트 무선통신장치로 경고 메시지를 자동으로 발송하고 치료 여부를 확인한 후 월 백신(300)을 자동으로 발송하는 것에 대한 간단한 블록도이다.

백신 개발자(405)는 1차 감염자(410)로부터 월 바이러스 정보를 수신하는 월 바이러스 수신부(615)와, 월 바이러스 여부를 확인하는 월 바이러스 검색부(610), 상기 월 바이러스를 치료하는 백신 및 상기 월 바이러스 전파 경로를 추출하는 월, 상기 백신 개발자와 상호 연결하는 백도어로 구성되는 월 백신(300)을 전송하는 월 백신 전송부(620). 상기 백도어를 관리하는 백도어 관리부(650) 및 상기 월 바이러스 감염자에 설치된 백도어로부터 월 바이러스 전파 경로에 대한 정보를 수신하는 백도어 수신부(655), 상기 전파 경로에 대한 정보를 참조하여 E-mail사(425)와 연동하여 각 E-mail주소에 해당하는 무선통신장치 번호를 생성하는 무선통신장치 번호 생성부(605), 신종 월 바이러스에 대한 경고 메시지를 자동으로 생성하는 월 바이러스 경고 메시지 생성부(625), 그리고 월 바이러스 경고 메시지를 월 바이러스 감염자의 무선통신장치로 발송하여 치료 여부를 확인하는 경고 메시지 발송부(635), 월 바이러스 감염자의 무선통신장치로부터 치료 여부를 수신하는 무선 데이터 수신부(640) 등으로 구성된다.

월 바이러스 수신부(615)는 1차 감염자(410)로부터 전송되는 월 바이러스 정보를 수신하는 역할을 수행하며, 이 때 월 바이러스 수신부(615)가 수신하는 월 바이러스 정보는 월 바이러스 종류에 따라 다르다. 예를 들어, 메일에 첨부된 형태의 월 바이러스라면, 월 바이러스 수신부(615)는 월 바이러스 정보를 전자 우편의 형태로 수신하며, P2P 시스템을 기반으로 하는 월 바이러스라면, P2P 송수신 데이터의 형태로 월 바이러스 정보를 수신한다. 또한 월 바이러스 경고 메시지에 대한 월 바이러스 감염자의 치료에 대한 확인 여부의 메시지도 수신한다.

월 바이러스 검색부(610)는 월 바이러스 수신부(615)에 의해 수신된 월 바이러스가 실제로 인터넷 상에서 자동 전파되는 월을 포함하고 있는지 확인한 후, 월을 포함하고 있는 경우에 대하여 신종 월 바이러스 여부를 결정하고, 신종 월 바이러스로 확인된 경우에 대하여 월 바이러스 공식 명칭을 자동으로 할당하며, 해당 월 바이러스의 특징을 분석하여 보고서를 자동 생성한다. 이렇게 생성된 보고서는 월 백신 개발자(405)의 프로그래머들이 월 백신(300)을 빠르게 개발하는 것에 사용될은 물론, 신종 월 바이러스 경고 메시지 생성부(635)에서 경고 메일에 월 바이러스에 대한 자세한 정보를 포함하는데 사용된다.

월 백신 전송부(620)는 상기 월 바이러스 검색부(610)의 검색결과를 참조하여 생성된 백신과 상기 월 바이러스 전파 경로를 추출하는 월과 상기 백신 개발자(405)와 상호 연결하는 백도어를 포함하여 구성되는 월 백신(300)을 상기 1차 감염자(410)에게 전송하는 역할을 수행한다.

또한, 상기 월 백신 전송부(620)는 하기에서 기술되는 월 바이러스 감염자의 무선통신장치로 발송하여 치료 여부를 확인하는 경고 메시지 발송 후 치료 여부가 확인된 월 바이러스 감염자에게 상기 월 백신(300)을 전송하는 역할을 수행한다.

또한, 상기 월 백신(300)은 월 백신(300) 내 월의 자가 복제를 통해 월 백신(300)이 상기 월 바이러스의 전파 경로로 전송되는 경우, 상기 월 바이러스의 전파 경로를 추적하여 추적 경로에 위치하는 클라이언트 무선통신장치로 상기 월 바이러스 경고 메시지를 전송한 후 상기 경고 메시지를 수신한 클라이언트 무선통신장치로부터 치료여부에 대한 응답 결과를 상기 백신 개발자로부터 전송 받아 상기 월의 자가 복제를 통한 상기 월 백신(300)의 전송 경로를 선택적으로 선별하여 전송하도록 하는 명령 수신부(Order Receiver)를 더 포함하여 구성될 수도 있음을 명기하는 바이다.

백도어 수신부(640)는 상기 월 백신(300)이 상기 1차 감염자 시스템에 설치한 백도어를 통해 월 바이러스에 대한 정보 및 월 바이러스 전파경로를 수신한다.

백도어 관리부(650)는 백도어 D/B(665)를 통해 월 백신(300)이 월 바이러스 감염자에 설치한 백도어들을 관리하고, 백도어 수신부(655)를 통해 월 바이러스 감염자로부터 수신된 정보 등을 분석하고, 이것을 바탕으로 하기에서 기술되는 신종 월 바이러스 경고 메시지 생성부(625)에서 생성된 경고 메시지를 생성하도록 한다.

백도어 관리부(650)의 백도어 D/B(665)에는 월 바이러스 경고 메일이 월 바이러스 감염자에 설치한 백도어에 대한 정보, 백도어 수신부(655)에서 확인된 월 바이러스 전파 경로 정보, 그리고 월 바이러스 감염자들에게 발송된 월 바이러스 경고 메시지 정보 등이 저장되어 있다.

2차-N차 월 바이러스 감염자 무선통신장치 번호 생성부(605)는 사전 약정에 의해 각 E-mail사(425)와 연동하여 상기 월 바이러스 전파 경로에 위치하는 월 바이러스 감염자의 각 E-mail에 해당하는 전화번호를 생성하며, 월 바이러스 감염자들의 무선통신장치로 즉각적으로 감염사실을 알리기 위해 경고 메시지가 발송될 2차에서 N차까지의 감염자 무선통신장치 번호를 생성한다.

여기서, 상기 월 바이러스 감염자 무선통신장치 번호 생성부(605)가 각 E-mail사(425)와 연동하여 2차 감염자 무선통신장치 전화번호를 다운받는 것은 본 발명 구현의 간소화를 위한 것이며(각 E-mail사(425)는 E-mail 회원정보에 사용자 무선통신장치 번호를 기 저장하고 있으므로), 상기와 같이 2차 감염자 무선통신장치 전화번호 추출은 상기 1차 감염자로부터 별도로 제공받거나 사전 서비스 제공을 위해 상기 1차 감염자 시스템내 이메일주소와 연동하는 무선통신장치 전화번호를 기 저장후 상기 주소록으로부터 상기 월 백신(300)에 의해 생성 가능한 바를 명기하는 바이다.

신종 월 바이러스 경고 메시지 생성부(625)는 신종 월 바이러스 1차 감염자가 확인된 경우 피해를 최소화하기 위해 즉각적으로 2차-N차 월 바이러스 감염자 무선통신장치 번호 생성부(605.5)의 정보를 기반으로 2차 월 바이러스 감염자에의 무선통신장치로 감염사실을 알리고 치료 여부를 확인하기 위한 경고 메시지를 생성한다.

신종 월 바이러스 경고 메시지 발송부(635)는 월 바이러스 2차-N차 감염자의 무선통신장치로 상기 월 바이러스 경고 메시지 생성부(625)를 통해 생성된 경고 메시지를 각 이동통신사를 통해 차-N차 월 바이러스 감염자 무선통신장치로 발송하는 역할을 담당한다.

무선 데이터 수신부(640)는 상기 월 바이러스 감염자의 무선통신장치로부터 치료 여부를 수신하는 역할을 수행하며, 치료 여부에 따라 상기 월 백신 전송부(620)로 하여금 월 백신(300)을 전송하도록 한다.

여기서, 상기 월 백신(300)내 월의 자가 복제를 통해 월 백신(300)이 상기 월 바이러스의 전파 경로로 전송되는 경우에는 상기 경고 메시지를 수신한 클라이언트 무선통신장치로부터 치료여부에 대한 응답 결과를 상기 무선 데이터 수신부로부터 상기 월 백신(300)내 명령 수신부(Order Receiver)로 전송하고, 상기 월 백신(300)내 명령 수신부(Order Receiver)에 의하여 상기 월 백신(300)의 전송 경로를 선택적으로 선별하여 월의 자가 복제를 통해 생성된 월 백신(300)을 자동 전송하도록 한다.

도면7은, 월 바이러스 1차 감염자(백신제공자에게 월 바이러스 감염 여부를 문의하는 클라이언트를 의미하며, 본 발명에서 추구하는 월 바이러스 경고메일 및 월 백신(300) 자동 배포의 시발점 역할을 수행하는 클라이언트)(410)로부터 상기 월 바이러스 전파 경로(상기 월 바이러스에 감염된 시스템상의 이메일 주소록 및 받은 편지함, 보낸 편지함, 지운 편지함 등에서 추출한 이메일 주소를 통해 상기 월 바이러스가 송·수신된 경로를 말하며, 상기 월 바이러스에 감염된 시스템으로부터 상기 월 바이러스를 전송받은 월 바이러스 숙주 시스템 및 상기 월 바이러스에 감염된 시스템으로부터 상기 월 바이러스를 전송받은 월 바이러스 수신 시스템의 이메일 주소를 총칭함)를 추출 및 상기 전파 경로에 위치하는 클라이언트 무선통신장치로 경고 메시지를 자동으로 발송하고 치료 여부를 확인한 후 월 백신(300)을 자동으로 발송하는 것에 대한 간단한 흐름도이다.

월 바이러스 경고 시스템(600)의 월 바이러스 수신부(615)에 월 바이러스 1차 감염자(410)로부터 월 바

이러스에 대한 정보가 수신되면(700), 웜 바이러스 검색부(610)는 수신된 웜 바이러스에 웜이 존재하는지 확인한다(705). 웜 바이러스 검색부(610)에서 수신된 웜 바이러스에 웜이 존재하는지 확인하는 방법은, 웜 바이러스 검색부(610)의 모든 네트워크 통신을 일시 차단한 상태에서, 웜 바이러스 검색부(610)가 수신된 웜 바이러스에 직접 감염된 후, 외부로 전송되는 패킷 데이터를 분석함으로서 웜의 존재 여부를 자동 확인 한다.

웜 검색부(610)는 상기와 같이 웜 바이러스에 직접 감염되어 패킷 데이터를 분석하여 웜의 존재 여부를 확인하기 때문에, 웜 바이러스 경고 시스템(600)의 다른 구성요소 및 웜 바이러스 백도어 시스템(645)과 다른 독립된 시스템에 구현한다.

만일 웜이 존재한다면(710) 상기 웜 검색부(610)는 신종 웜 바이러스인지를 확인하게 되고(715), 신종 웜 바이러스로 확인된 경우에 대하여(725) 웜 바이러스 공식 명칭을 자동으로 할당하고(730), 해당 웜 바이러스의 특징을 분석하여 보고서를 자동 생성한다(740).

상기 웜 바이러스 검색부(610)의 검색결과를 참조하여 상기 웜 바이러스에 대한 백신 개발 후, 웜 백신 전송부(620)는 상기 웜 바이러스 치료 백신과 상기 웜 바이러스 전파 경로를 추출하는 웜과 상기 백신 개발자(405)와 상호 연결하는 백도어를 포함하여 구성되는 웜 백신(300)을 상기 1차 감염자(410)에게 전송한다.

상기 1차 감염자(410)에 수신된 상기 웜 백신의 백신은 상기 1차 감염자(410)의 웜 바이러스를 치료하며(745), 상기 웜은 상기 1차 감염자(410)로부터 웜 바이러스 전파 경로를 추출하고, 상기 1차 감염자(410)에 백도어를 설치한다. 상기 1차 감염자(410)로부터 추출된 웜 바이러스 전파 경로는 상기 백도어를 통해 상기 백신 개발자(405)의 백도어 수신부(655)로 전송되고, 상기 웜 바이러스에 대한 정보 및 웜 바이러스 전파경로를 수신한 백도어 수신부(655)는 상기 백도어를 관리하는 백도어 관리부(650)로 데이터를 전송한다(750).

백도어 관리부(650)는 상기 백도어 수신부(655)를 통해 웜 바이러스 감염자로부터 수신된 정보 등을 분석하고, 이것을 바탕으로 하기에서 기술되는 신종 웜 바이러스 경고 메시지 생성부(625)에서 생성된 경고 메시지를 생성하도록 한다(740).

상기 백도어 관리부(650)로부터 수신된 웜 바이러스 전파 경로 데이터를 기반으로 2차~N차 웜 바이러스 감염자 무선통신장치 번호 생성부(605)로 하여금 사전 약정에 의해 각 E-mail사(501)와 연동하여 (755) 상기 웜 바이러스 전파 경로에 위치하는 웜 바이러스 감염자의 각 E-mail에 해당하는 전화번호를 생성하며, 웜 바이러스 감염자들의 무선통신장치로 즉각적으로 감염사실을 알리기 위해 경고 메시지가 발송될 2차에서 N차까지의 감염자 무선통신장치 번호를 생성한다(760).

여기서, 상기 웜 바이러스 감염자 무선통신장치 번호 생성부(605)가 각 E-mail사(425)와 연동하여 2차 감염자 무선통신장치 전화번호를 다운받는 것은 본 발명 구현의 간소화를 위한 것이며(각 E-mail사(425)는 E-mail 회원정보에 사용자 무선통신장치 번호를 기 저장하고 있으므로), 상기와 같이 2차 감염자 무선통신장치 전화번호 추출은 상기 1차 감염자(410)로부터 별도로 제공받거나 사전 서비스 제공을 위해 상기 1차 감염자 시스템내 이메일주소와 연동하는 무선통신장치 전화번호를 기 저장후 상기 주소록으로부터 상기 웜 백신(300)에 의해 생성 가능한 바를 명기하는 바이다.

상기 백도어 관리부(650)로부터 수신된 웜 바이러스 정보 데이터를 기반으로 신종 웜 바이러스 경고 메시지 생성부(625)는 신종 웜 바이러스 1차 감염자(410)가 확인된 경우 피해를 최소화하기 위해 즉각적으로 상기 2차~N차 웜 바이러스 감염자 무선통신장치 번호 생성부(605)에서 생성된 감염자 무선통신장치 번호로 감염사실을 알리고 치료 여부를 확인하기 위한 경고 메시지를 생성한다(765).

상기 생성된 경고 메시지는 신종 웜 바이러스 경고 메시지 발송부(635)를 통해 각 이동통신사(430)를 통해 상기 웜 바이러스 2차~N차 감염자의 무선통신장치로 발송한다(770).

상기 경고 메시지를 수신한 클라이언트는 경고 메시지를 문자 서비스를 통해 보게되며(775), 웜 바이러스 치료 여부에 대해 확인을 요청하게 되고(780), 거절하면 서비스는 종료된다(790).

웜 바이러스 치료 여부에 대한 확인에 치료를 요청하게 되면, 무선 데이터 수신부(640)를 통해 상기 웜 바이러스 감염자의 무선통신장치로부터 치료 여부를 수신한 후, 상기 웜 백신 전송부(620)로 하여금 상기 치료 여부 승인 감염자에게 웜 백신(300)을 전송하도록 한다(785).

여기서, 상기 웜 백신(300)내 웜의 자가 복제를 통해 웜 백신(300)이 상기 웜 바이러스의 전파 경로로

전송되는 경우에는 상기 경고 메시지를 수신한 클라이언트 무선통신장치로부터 치료여부에 대한 응답 결과를 상기 무선 데이터 수신부(640)로부터 상기 월 백신(300)내 명령 수신부(Order Receiver)(310)로 전송하고, 상기 월 백신(300)내 명령 수신부(Order Receiver)(310)에 의하여 상기 월 백신(300)의 전송 경로를 선택적으로 선별하여 월의 자가 복제를 통해 생성된 월 백신(300)을 자동 전송하도록 한다.

상기 치료 여부 승인 감염자에게 전송된 월 백신(300)은 월과 백도어를 통해 상기와 같은 각 단계들을 반복하여 월 바이러스를 말살한다.

도면8은 외부와 차단된 가상 네트워크 안에서 월을 찾는 월 바이러스 검색부(610)에 대한 간단한 블록도이다.

월 바이러스 검색부(610) 월 바이러스 검색 장치와 네트워크 차단 장치로 구성되어 있으며, 월 바이러스 검색 장치는 가상으로 존재하는 주소록과 편지함들을 가지고 있는 독립 컴퓨터 시스템이다. 월 바이러스 검색 장치는 월 바이러스에 직접 감염되기 전에 LAN(Local Area Network)과 WAN(Wide Area Network)을 포함하는 실제 네트워크와 완전 차단(허브 또는 게이트웨이와 소프트웨어적은 물론 하드웨어적으로 완전 단절)된 후, 내부의 가상 네트워크를 통해 패킷 데이터를 분석한다.

네트워크 차단 장치는 월 바이러스 검색부(610)와 실제 네트워크를 완전 차단하며, 월 바이러스 검색 장치가 월을 검색하는 과정을 모니터링한다. 네트워크 차단 장치는 소프트웨어적인 형태로 제작되거나, 하드웨어적인 방법으로 제작되며, 경우에 따라 소프트웨어적인 방법과 하드웨어적인 방법을 결합하여 제작되기 때문에, 월 바이러스의 감염 대상이 아니다. 따라서 월 바이러스 검색 장치가 월 바이러스에 감염되어 시스템에 치명적인 손상을 입더라도, 네트워크 차단 장치는 월 바이러스 검색 장치로부터 월의 존재 여부를 모니터링할 수 있다.

월 바이러스 검색부(610)는 상기와 같은 방법을 통해 수신된 월 바이러스에서 월이 존재 여부를 확인한 후, 해당 월 바이러스에 월이 존재하지 않는다면, 월 바이러스 검색을 종료한다. 그러나 수신된 월 바이러스에 월이 존재가 확인되면, 월 바이러스 검색부(610)는 이것이 기존에 존재하는 월 바이러스인지, 아니면 신종 월 바이러스인지를 확인한다.

만약 기존에 존재하는 월 바이러스라면, 월 바이러스 검색부(610)는 월 바이러스 경고 메일 생성 작업을 수행하지 않고, 해당 월 바이러스에 대한 경고 시스템을 종료한다. 그러나 수신된 월 바이러스가 기존에 존재하지 않는 신종 월 바이러스라면, 월 바이러스 검색부(610)는 주어진 조건을 바탕으로 신종 월 바이러스의 공식 명칭을 할당하고, 이 월 바이러스에 대한 특징을 자동으로 분석하여 보고서를 작성한다.

월 바이러스 검색부(610)에서 신종 월 바이러스에 대한 보고서가 작성되면, 신종 월 바이러스 경고 메시지 생성부(625)는 월 바이러스 검색부(610)가 작성한 보고서를 바탕으로 신종 월 바이러스에 대한 월 백신(300) 및 경고 메시지를 생성한다.

도면9는 상기 치료 여부 확인 감염자에게 전송된 월 백신(300)의 월과 백도어를 통해 도면 7과 같은 각 단계들을 반복하여 월 바이러스를 말살하는 과정에 대한 간단한 흐름도이다.

상기 치료 요청 클라이언트(또는 2차 감염자) 시스템으로 전송된 월 백신은(900) 신종 월 바이러스 정보 및 경고 메시지를 출력한 후(905), 신종 월 바이러스의 차단 및 치료를 위해 백도어 설치 여부를 확인한다(910).

만약 상기 치료 요청 클라이언트 시스템이 백도어 설치를 승인하면(915), 월 바이러스 월 백신 메일은 해당 시스템에 백도어 설치를 시작한다(920). 그러나 반대로 백도어 설치를 거부하면, 월 바이러스 월 백신 메일은 월 바이러스 경고 시스템(600)으로 백도어 설치가 거부되었음을 전송한다(925).

상기 치료 요청 클라이언트 시스템에 백도어가 설치되면, 월 바이러스 월 백신 메일은 해당 시스템으로부터 월 바이러스가 전파 가능한 모든 경로(상기 월 바이러스에 감염된 시스템상의 이메일 주소록 및 받은 편지함, 보낸 편지함, 지운 편지함 등에서 추출한 이메일 주소를 통해 상기 월 바이러스가 송·수신된 경로를 말하며, 상기 월 바이러스에 감염된 시스템으로 상기 월 바이러스를 전송한 월 바이러스 숙주 시스템 및 상기 월 바이러스에 감염된 시스템으로부터 상기 월 바이러스를 전송받은 월 바이러스 수신 시스템의 이메일 주소를 총칭함)를 추출하여(930), 월 바이러스 전파 경로를 결정하고(935), 이것을 백도어를 통해 월 바이러스 백도어 시스템(645)으로 전송한다(940).

월 바이러스 백도어 시스템(645)의 백도어 수신부(655)가 월 바이러스 감염자에 설치된 월 바이러스 월 백신 메일의 백도어를 통해 월 바이러스의 전파 경로 경로를 수신하면, 백도어 관리부(650)는 이것을 백도어 O/B(665)에 저장하고(945), 월 바이러스 감염자 무선통신장치 번호 생성부(605)에서 각 전파 경로에 대한 감염자 무선통신장치 번호를 전송 받음과(950) 동시에 신종 월 바이러스 경고 메시지 생성부(615)가 생성한 경고 메시지를 감염자의 무선통신장치로 발송한다(955). 월 바이러스 감염자에게

치료 여부를 확인하여(960) 거절하면 서비스는 종료된다(965). 월 바이러스 감염자가 무선통신장치 상에서 서비스를 요청하게 되면(확인키를 누름)(970) 상기 월 바이러스 감염자 시스템으로 신종 월 바이러스 월 백신 메일을 발송한다(975). 이 과정은 반복적으로 수행되고 월 백신 메일 발송이 완료되면 월 바이러스 월 백신 메일 발송 결과를 저장한다(980).

도면 10은 월 백신 개발자(405)로부터 백신 메일링 서비스 요청자 또는 월 바이러스 1차 감염자(410)에게 전송된 월 백신(300)이 월 바이러스를 치료하고 있는 간단한 예시도이다.

월 백신(300)이 월 백신 개발자(405)로부터 백신 메일링 서비스 요청자 또는 1차 월 바이러스 감염자(410)에게 전송되면(1000), 월 백신(300)은 메일 클라이언트 프로그램의 모든 작업을 차단하고, 월 바이러스 검색을 시작한다(1005).

이 때 월 백신(300)은 목표로 하는 월 바이러스는 물론, 기존에 존재하는 다른 월 바이러스와 클라이언트 바이러스를 포함하여, 시스템에 악영향을 미치고 있는 스파이웨어 등을 검색하고, 월 바이러스가 전파된 경로를 추출한다.

월 백신(300)을 통해 목표로 하는 신종 월 바이러스 및 기존에 존재하는 다른 종류의 월 바이러스가 발견되면(1010), 월 백신(300)은 해당 월 바이러스의 전파 경로를 추출하고(1015), 발견된 모든 종류의 바이러스와 스파이웨어를 제거하고(1020), 변경된 시스템을 원래 상태로 복구한다(1025).

치료 과정에서 월 백신(300)은 사용자에게 목표로 하는 신종 월 바이러스의 자세한 정보 등을 바이러스 치료 화면에 출력시키거나, 광고를 노출시키는 부가 서비스를 함께 제공한다.

도면 11은 2차 월 바이러스 감염자(415)의 무선통신장치로 월 바이러스 감염 사실을 알리고 치료 여부를 확인하는 경고 메시지 발송의 일실시예도이다.

발명의 효과

본 발명에 따르면, 인터넷 또는 전자 우편 시스템에서의 월 바이러스 최초 탐지 후, 월 바이러스 백신 제작자에 의해 해당 월 바이러스의 전파 경로를 추적하여 추적 경로에 위치하는 클라이언트 무선통신장치로 상기 월 바이러스에 대한 경고 메시지를 자동 전송 및 치료여부를 확인함으로써, 상기 월 바이러스에 의한 감염을 최소화하는 효과가 있으며, 월 바이러스에 의한 경제적 피해를 최소화 할 수 있는 효과가 있다.

또한, 본 발명에 따르면 상기 월 바이러스의 전송 범위(시스템에서 시스템으로 기하 급수적으로 팽창되는 범위)와 동일한 범위를 통해 전파되는 상기 월 바이러스에 대한 경고 메시지 및 월 백신에 광고를 삽입하여 제공함에 따라 단시간내 가장 큰 효과를 볼 수 있는 광고 방법을 제공하는 효과가 있다.

(57) 청구의 범위

청구항 1

월 바이러스 발견 또는 감염된 클라이언트 시스템으로부터 전송된 월 바이러스 정보 데이터를 수신하는 제 1단계;

상기 월 바이러스 정보 데이터를 참조하여 상기 월 바이러스를 치료 및 상기 월 바이러스 전파 경로를 추적하는 월이 첨부된 월 백신을 상기 클라이언트 시스템으로 전송하는 제 2단계;

상기 월 백신을 이용하여 상기 월 바이러스를 치료 및 상기 클라이언트 시스템에 백도어를 설치하는 제 3단계;

상기 월 백신을 이용하여 상기 클라이언트 시스템상의 상기 월 바이러스 전파 경로를 추출 및 상기 백도어를 통해 상기 월 백신 제공 서버로 상기 월 바이러스 전파 경로 데이터를 전송하는 제 4단계;

상기 월 바이러스 전파 경로 데이터를 참조하여 상기 월 바이러스 전파 경로에 위치하는 클라이언트 각 E-mail에 해당하는 무선통신장치 전화번호를 생성하는 제 5단계;

상기 생성된 무선통신장치 번호로 경고 메시지-상기 월 바이러스 전파 정보 및 치료 여부를 확인하는 메시지를 전송하는 제 6단계; 및

상기 무선통신장치로부터 치료 여부 승인 데이터를 수신한 후, 상기 치료 여부 승인 클라이언트에게 상기 월 백신을 전송하는 제 7단계;를 포함하여 이루어지는 것을 특징으로 하는 무선 월 바이러스 경고 메시지 자동 발송 방법.

청구항 2

1항에 있어서, 상기 웜 바이러스가 전파 가능한 경로를 추출하는 제 4단계는,

상기 메일 클라이언트 시스템의 이메일 주소록과 받은 편지함, 보낸 편지함, 그리고 클라이언트가 방문하는 인터넷 웹사이트와 FTP 사이트를 참조하여 상기 웜 바이러스가 전파 가능한 경로를 추출하는 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 방법

청구항 3

제 1항에 있어서, 상기 무선통신장치 전화번호를 생성하는 제 5단계는,

각 E-mail사와 연동하여 상기 웜 바이러스 전파 경로에 위치하는 클라이언트 각 E-mail에 해당하는 무선통신장치 전화번호를 생성하는 방법; 또는

상기 웜 바이러스 발견 또는 감염된 클라이언트 시스템과의 양방향 통신을 통해 직접 제공받아 생성하는 방법; 또는

상기 웜 바이러스 발견 또는 감염된 클라이언트 시스템내 이메일주소와 연동하는 무선통신장치 전화번호를 기 저장후 상기 주소록으로부터 상기 웜 백신에 의해 자동 생성하는 방법;을 포함하여 이루어지는 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 방법

청구항 4

제 1항에 있어서, 상기 웜 백신 자동 전파 방법은,

자가(Native) 전파, 또는 기생(Parasitic) 전파, 또는 독단 프로토콜(Arbitrary Protocol) 전파, 또는 P2P(Peer-to-Peer) 전파를 이용하는 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 방법

청구항 5

제 1항에 있어서, 상기 치료 여부 승인 클라이언트에게 상기 웜 백신을 전송하는 제 7단계는,

상기 무선통신장치로부터 수신한 치료 여부 승인 데이터를 상기 웜 바이러스 발견 또는 감염된 클라이언트 시스템내 웜 백신으로 송신하여 상기 웜 백신내 웜의 자가복제를 통해 상기 치료 여부 승인 클라이언트 시스템으로 자동 전송하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 방법.

청구항 6

웜 바이러스 발견 또는 감염된 클라이언트 시스템으로부터 웜 바이러스 정보 데이터를 수신하는 웜 바이러스 수신부;

상기 웜 바이러스 수신부를 통해 수신된 상기 웜 바이러스 정보 데이터를 확인하여 웜 바이러스 존재 여부를 검색하는 웜 바이러스 검색부;

상기 웜 바이러스 검색부의 검색결과를 참조하여 생성된 백신과 상기 웜 바이러스 전파 경로를 추출하는 웜과 상기 백신 개발자와 상호 연결하는 백도어를 포함하여 구성되는 웜 백신을 상기 클라이언트 시스템으로 전송하는 웜 백신 전송부;

상기 웜 백신이 설치한 상기 클라이언트 시스템내 백도어로부터 상기 웜 바이러스 전파 경로에 대한 정보 데이터를 수신하는 백도어 수신부;

상기 백도어 수신부로 수신된 상기 웜 바이러스 전파 경로에 대한 정보 데이터를 기반으로 상기 웜 바이러스 전파 경로에 위치하는 클라이언트 각 E-mail에 해당하는 전화번호를 생성하는 무선통신장치 번호 생성부;

상기 무선통신장치로 감염사실을 알리고 치료 여부를 확인하기 위한 경고 메시지를 생성하는 경고 메시지 생성부;

상기 경고 메시지 생성부에서 생성된 경고 메시지를 각 이동통신사를 통해 상기 웜 바이러스 전파 경로에 위치하는 클라이언트 무선통신장치로 발송하는 경고 메시지 발송부; 및

상기 무선통신장치로부터 웜 바이러스 치료 여부 승인 데이터를 수신하는 역할을 수행하며, 치료 여부 승인에 따라 상기 웜 백신 전송부로 하여금 상기 치료 여부 승인 클라이언트 시스템으로 웜 백신을 전송하도록 하는 무선 데이터 수신부;를 구비하여 이루어지는 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 시스템.

청구항 7

제 6항에 있어서, 상기 웜 바이러스 검색부는,

상기 웜 바이러스 검색부와 연결되는 모든 네트워크 통신을 일시 차단한 상태에서, 상기 웜 바이러스 검

색부가 수신된 웜 바이러스에 직접 감염된 후, 외부로 전송되는 패킷 데이터를 분석함으로서 웜 바이러스의 존재 여부를 자동 확인하는 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 시스템.

청구항 8

제 6항에 있어서, 상기 웜 백신의 웜은,

상기 클라이언트 시스템에 존재하는 SMTP를 이용하거나, 또는

상기 웜 바이러스 경고 메일 또는 상기 웜 백신 내부에 내장된 SMTP를 이용하여,

상기 추출된 웜 바이러스 전파 경로를 향해 원본 웜 백신을 자가복제하여 재배포하는 기능을 구비하는 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 시스템.

청구항 9

제 6항에 있어서, 상기 웜 백신은,

무선 데이터 수신부가 수신한 치료 여부 승인 데이터를 수신하여 상기 웜 백신의 자가 복제 전송경로를 선택적으로 선별하여 전송하도록 하는 명령 수신부(Order Receiver)를 더 구비하여 이루어지는 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 시스템.

청구항 10

제 1항 또는 제 6항에 있어서,

상기 웜 바이러스를 일반 바이러스 또는 스파이웨어로 대체 가능한 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 방법 및 시스템.

청구항 11

제 1항 또는 제 6항에 있어서,

상기 웜 바이러스 경고 메시지 또는 웜 백신에 광고를 삽입하여 제공하는 것을 특징으로 하는 무선 웜 바이러스 경고 메시지 자동 발송 시스템.

청구항 12

제 1항 또는 제 6항에 있어서, 상기 전파 경로는,

상기 웜 바이러스에 감염된 시스템상의 이메일 주소록 및 받은 편지함, 보낸 편지함, 지운 편지함 등에서 추출한 이메일 주소를 통해 상기 웜 바이러스가 송·수신된 경로를 말하며, 상기 웜 바이러스에 감염된 시스템으로부터 상기 웜 바이러스를 전송한 웜 바이러스 숙주 시스템 및 상기 웜 바이러스에 감염된 시스템으로부터 상기 웜 바이러스를 전송받은 웜 바이러스 수신 시스템의 이메일 주소를 포함하는 것을 특징으로 하는 웜 바이러스 경고 메일 및 웜 백신 자동 발송 방법 및 시스템.

도면



월 바이러스가 포함된 메일

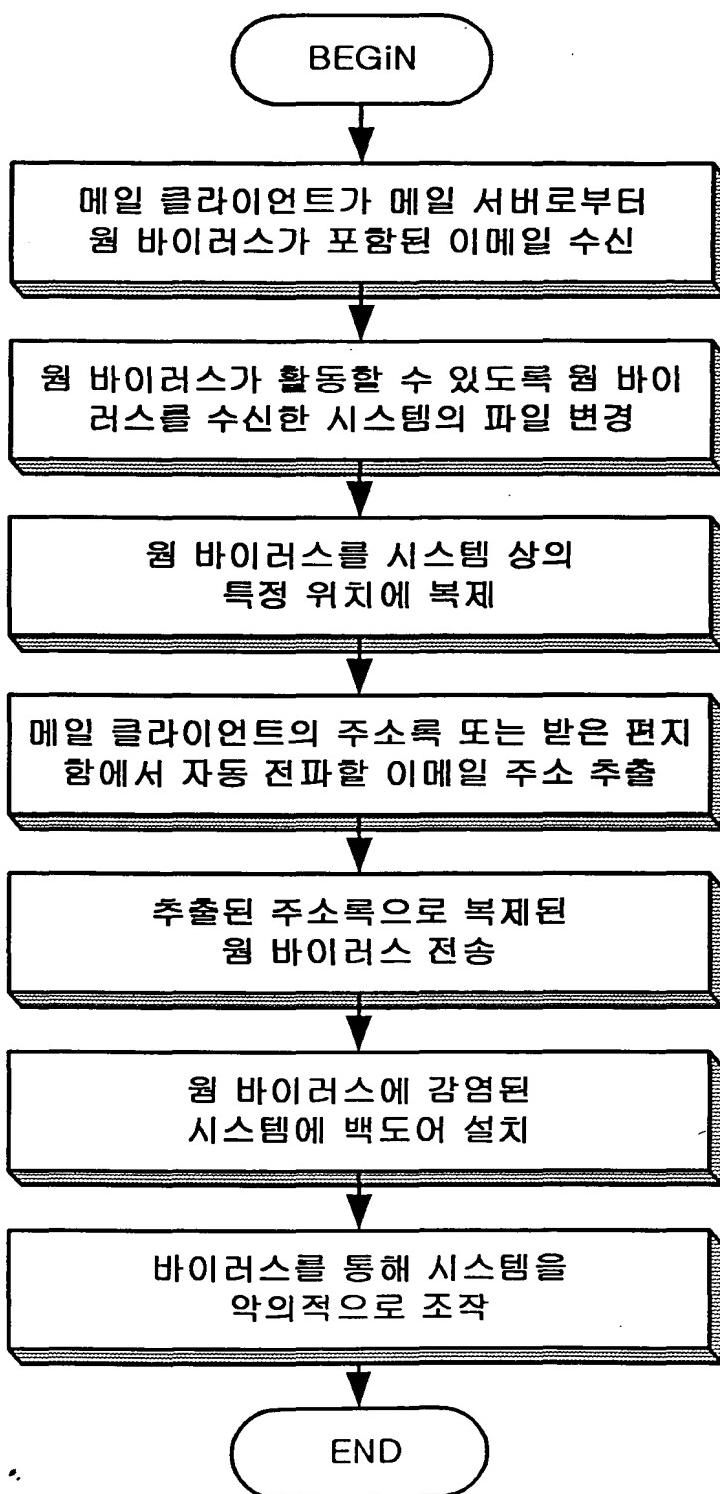
메일에 포함된 메시지

월 바이러스

VIRUS

WORM

BACK DOOR



월 백신이 포함된 메일

메일에 포함된 메시지

월 백신 (300)

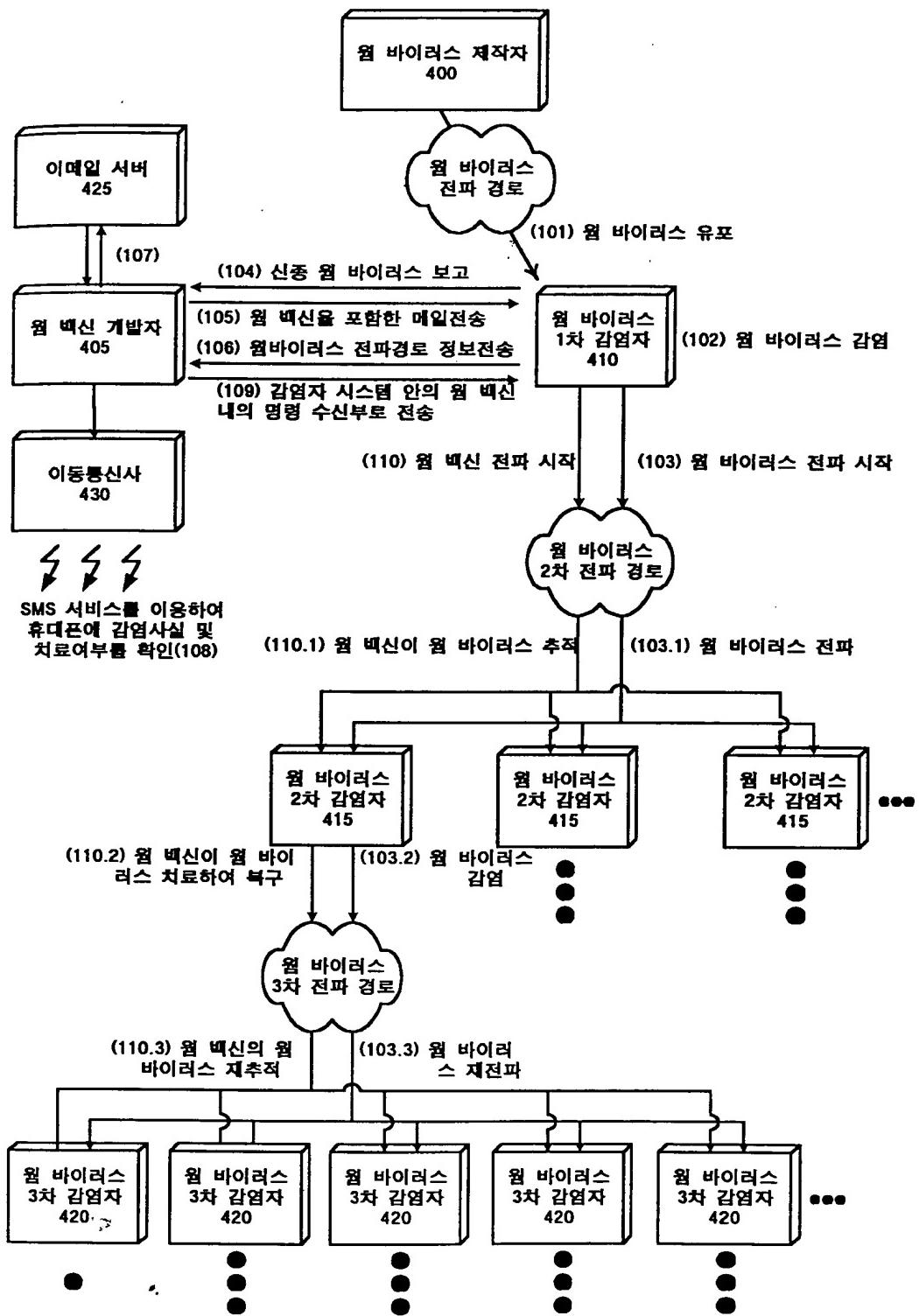
VACCINE
305

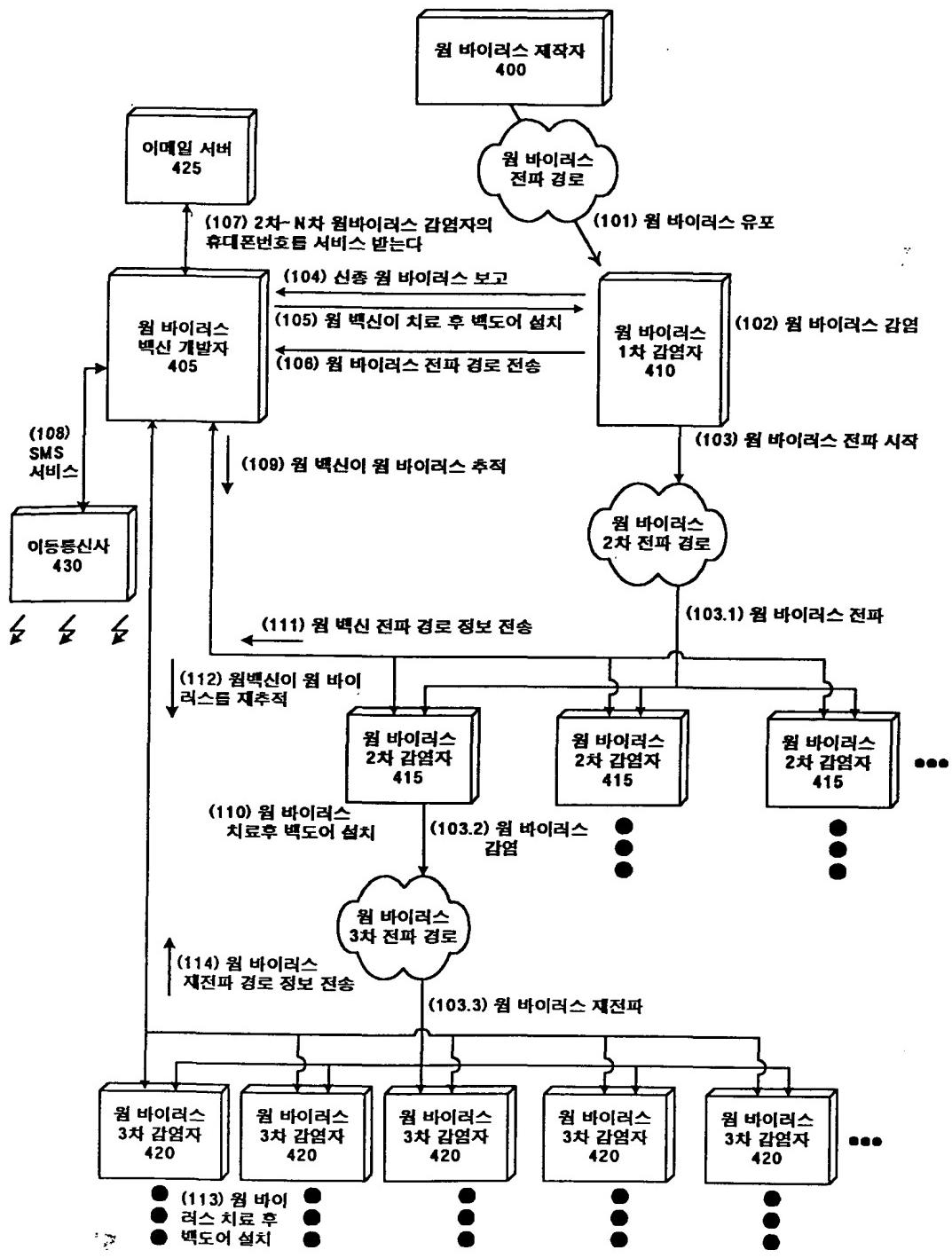
ORDER
RECEIVER (310)

BACK DOOR
320

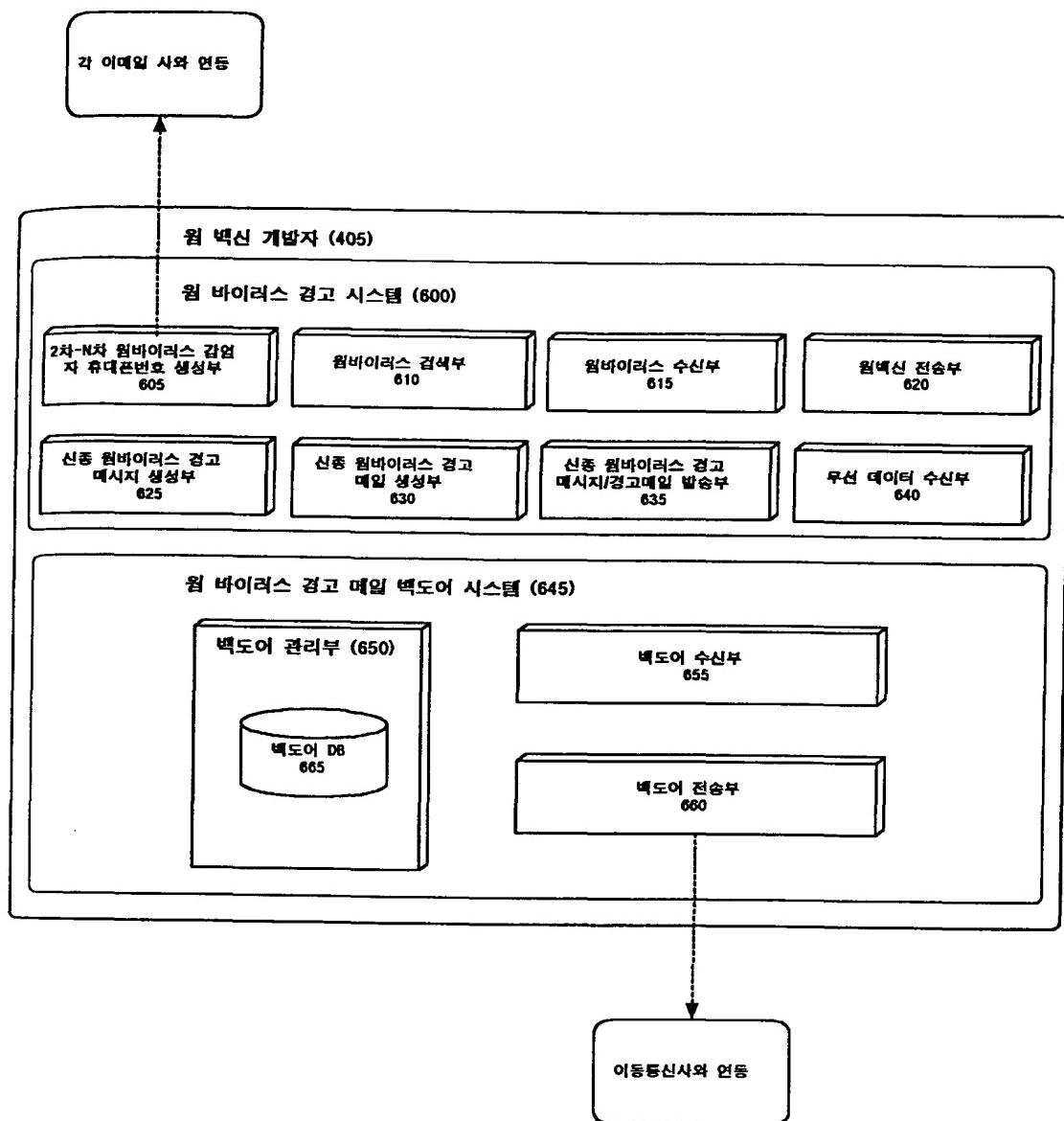
WORM
315

도면4

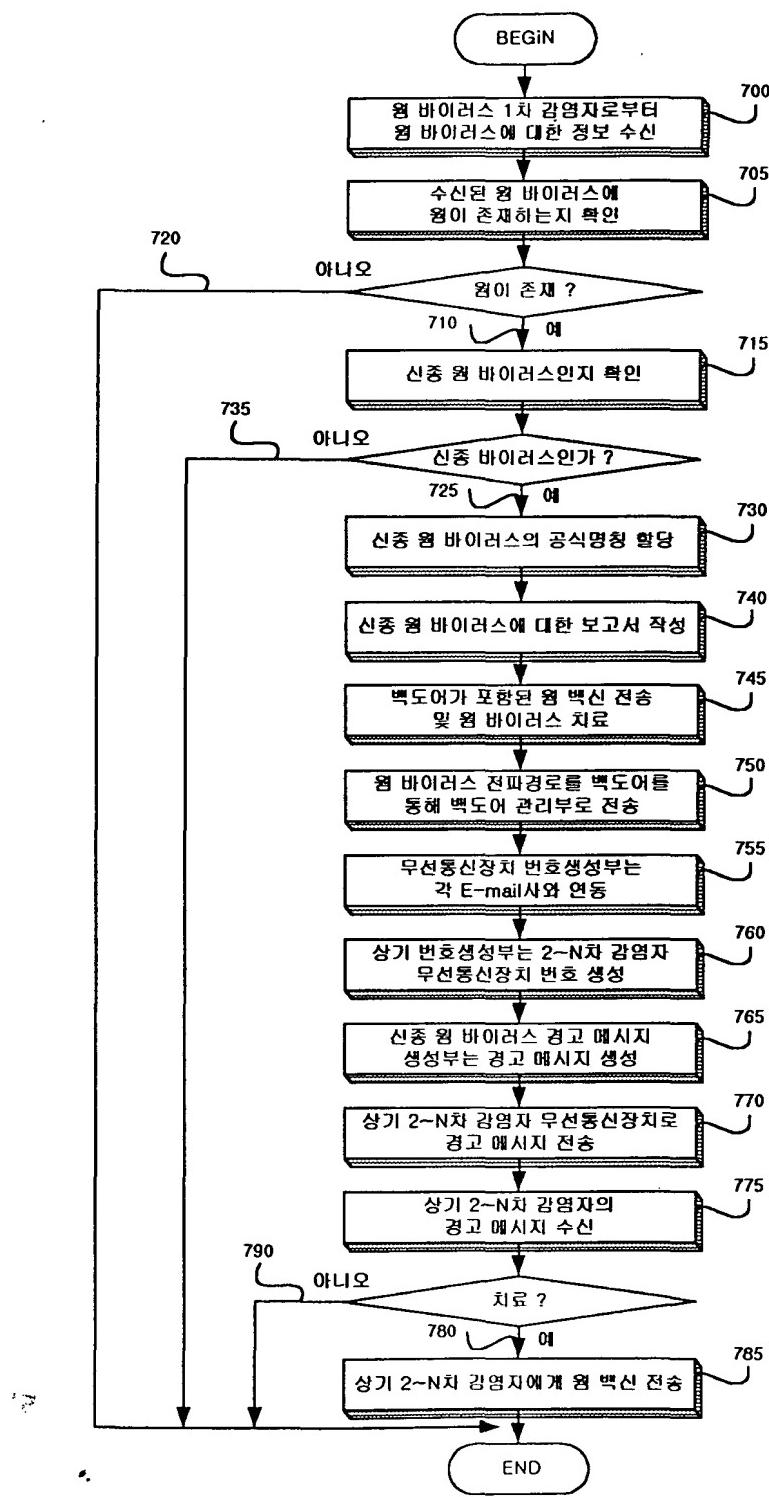




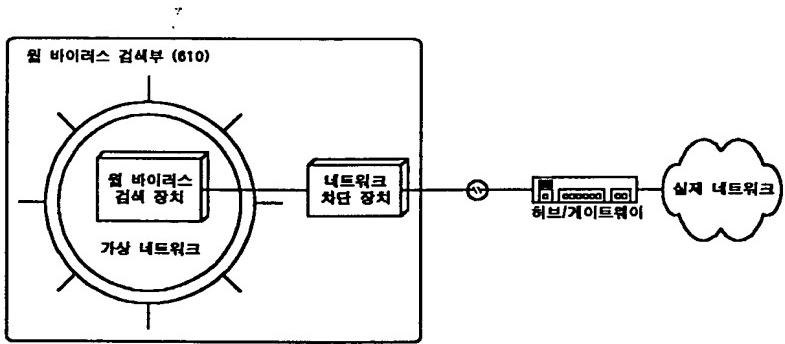
도면6



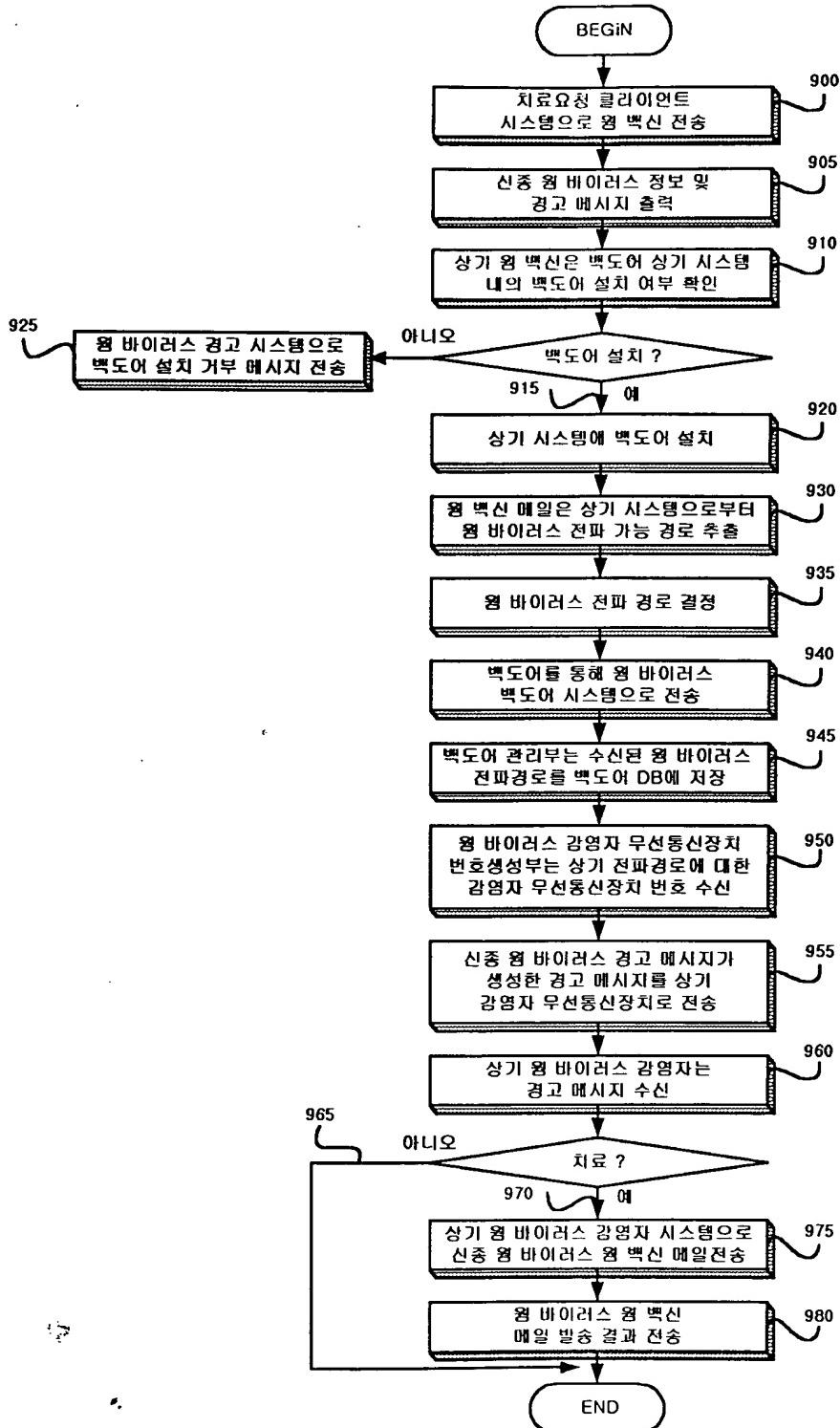
도면7



도면8

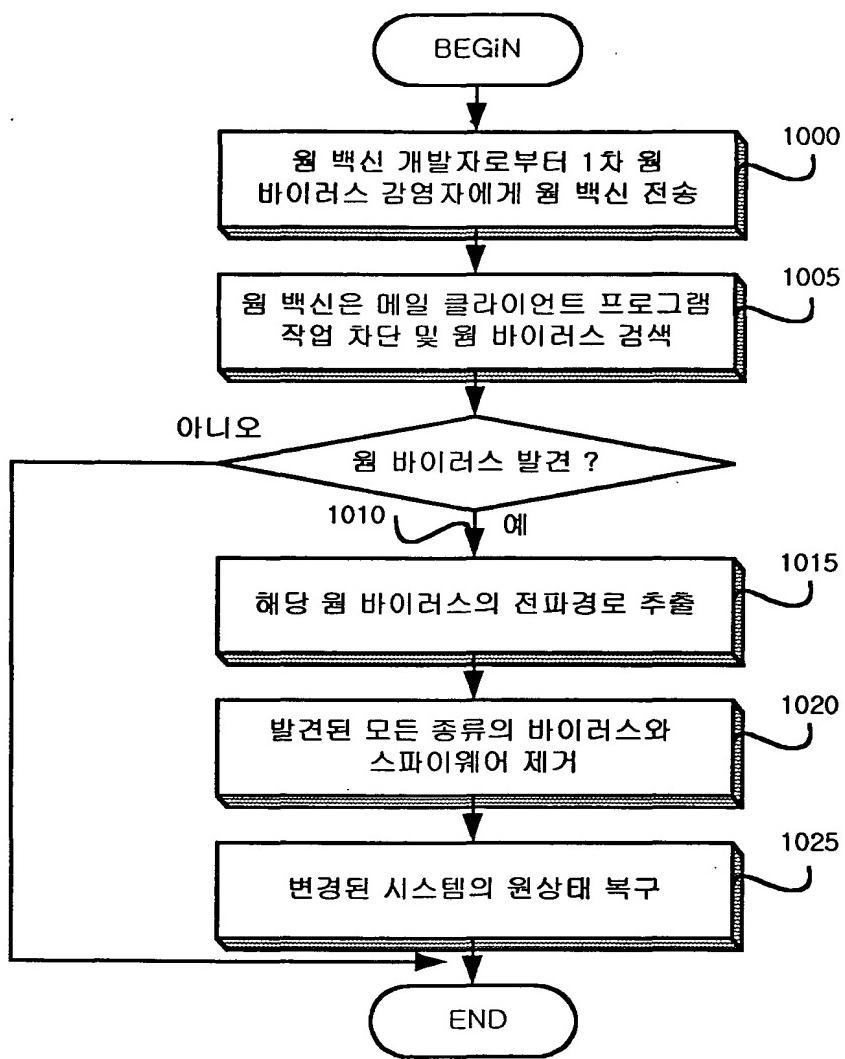


도면9



도면 10





도면11

경고 메시지 내용

신종 XXX월 바이러스에
감염되었습니다.
XXX에 특히 주의하시고
확인바랍니다.

치료를 원하시면 확인 키
를 눌러주세요!